Privacy and Security Audit Issues

R1.1
June 13, 2021

I3 Systems, 1146 N Central Ave #687, Glendale CA 91202
www.i3-iot.com

TABLE OF CONTENTS

Disclaimer: This document contains suggestions of issues which might be considered for possible inclusion in a potential privacy/security audit process. There may be other issues that are relevant to a company based on their targeted market, their local geography, or the geography of their customers. Readers are encouraged to use this document as a basis for conversation with their management, legal representatives, and their CIO/CTO/CDO as appropriate.

INTRODUCTION

During the first industrial revolution, companies sought to have direct control over everything that impacted their business. They sought to control the raw materials they needed to produce products, the supply chain, all aspects associated with manufacturing, and all the distribution channels. If the entire process could be controlled they could limit potential competitors and control market forces that shaped their supply and demand. Things have changed since then. As the world steadily marches toward the Fourth Industrial Revolution, organizations are finding that a network of affiliates and partners that interact with one another is better equipped to serve global markets where everyone is free to connect with each other over the Internet. Thus, as the world evolves, it has become clear that ecosystems will rule the future world rather than large companies that are vertically integrated. Superior economic growth is achieved when loosely coupled organizations work together to a common goal,

A myriad of research studies have shown that partnerships work best when there is sharing of data between participants. If partners exchange data, each partner can strive to achieve results that benefit the common cause. However, sharing of data will be reduced in situations where the partners do not trust one another. Thus trust is a critical issue when seeking to maximize partnership productivity.

Trust might be an easy topic to define as an interpersonal attribute but is a difficult concept to quantify in a business setting – especially when applied to data. At its most fundamental core, each organization has to evaluate whether the other organization intends to take advantage of and undermine the other organization. In many cases, trust requires the individuals involved in the partnership to be open and ethical, fully disclosing the nature of the relationship, the benefits, and the tactics to serve their common purpose.

Assuming this most basic level of trust can be met, there is a second level of trust that must be achieved for companies to feel secure in the exchange of data that enables the relationship to succeed. More specifically, both organizations have to consider whether the other organization is capable of ensuring that privileged data exchanged between organizations can be sufficiently protected by the organization. That is, if one organization believes the other organization bears no ill intent and data is exchanged, is the other organization capable of protecting the data from third parties who might also desire that data.

As a result, when two independent organizations seek to establish a trusted relationship between each other, the organizations must be able to demonstrate to each other that their organization is worthy of trust by the other organization. To do this, the organizations must be able to show the other organization that they are indeed capable of sufficiently protecting the data they receive from the other party. This is often done by an exchange of data policies. Data policies should document the steps each organization commits to supporting in order to protect the data that they hold. Both organizations should review the other company's data policy in order to make sure the other organization has sufficient safeguards in place to protect the data they hold.

A second requirement is for each of the two companies to review the other company's data privacy policies. Data security and data privacy are different but related concepts. Data security makes sure third parties have taken reasonable measures to ensure nefarious third parties do not have access to sensitive data. Data privacy are the policies that each company puts in place to make sure the data held by a company is not misused within the organization. Further, an organization cannot provide any assurances of privacy unless viable data security measures have been put in place.

RECOMMENDATIONS

The more an organization is trusted, the more their customers and partners will make data available to them. With greater amounts of data, the better an organization's decision making processes and the better their financial results. It is therefore in a company's best interest to treat 'trust' much like organizations treat quality. A quality driven organization regularly monitors the quality of their product and takes steps to improve quality given there are significant costs associated with poor quality. By the same token, companies should regularly monitor the factors that are associated with a trusted organization and take steps to improve the levels of trust between the organization and its customers and partners.

This implies that a company has a formal process that can be used to monitor efforts to provide data security and privacy. The organization should periodically self-audit their own practices against these metrics AND they should also audit their partners to make sure their partners are adequately protecting the data they receive.

As a service to its customers, I3 Systems has compiled the following list of best practices which an organization might consider including in their audit program. This list of potential considerations is long and therefore the recommendation is that an organization consider these issues for possible inclusion in their audit process while topics not included might become potential policy enhancement for implementation in future audits.

It is also noted that much like quality assurance processes have embraced the concept of continuous improvement, a similar concept should be adopted with data security/privacy. Yes, there are industry specific legal requirements that set a minimal baseline for security and privacy but legally enforced requirements should be treated as a starting point. Once this minimal level of achievement has been met, each year after that the organization should attempt to achieve more in an effort to maximize the benefits that are potentially possible in a data-driven environment.

MANAGEMENT AND GOVERNANCE ISSUES

An organization's privacy and security framework should be governed by a framework document. Such a master framework document points to the other policy and procedure documents that are part of the organization's management philosophy. To conduct an audit, the auditor will ensure that a framework document is in place and then can follow the links to the organization's policies and procedures to identify evidence of compliance. When an organization seeks to improve their policies and procedures, the changes should all be documented in a policy or procedure that is traceable back to the root framework document.

1.1	Does the organization have a data governance framework that includes and provides support for a data security and privacy policy?	A data governance framework defines all the policies and procedures that are associated with data privacy and security management. Some policies are externally visible (posted on the public internet) and some policies/procedures are intended as internal documents. Each policy is titled, dated, and formally approved. The data governance framework is the root document and creates a path to all other framework documents with details about when the other documents come to bear on a situation. The framework should not contain any orphan documents, documents that have no cause for activation.
1.2	Does the data governance framework include a partner code of conduct that partners are expected to follow?	If an organization shares data with a partner (or if it is sold, a customer) and that entity violates expected behaviors, the organization's data policies may be compromised. The data governance framework should require that all partnered companies commit their employees to conduct themselves according to expectations of the organization's framework when accessing/using the organization's data.
1.3	Does the organization have a single, consistent data privacy and security policy that applies to the entire organization? Any exceptions to these policies related to a specific project should be clearly defined in an explicit consent agreement.	The more different data policies an organization has, the harder it is for the organization to police and ensure compliance. The complexity of staff training on the company's values and principals also increases significantly with each new policy. Finally, when laws in this area change, efforts to implement the new procedures are more difficult when there are many different policies to coordinate between.
1.4	Does the organization have a defined data privacy policy that is supported by the entire management team?	Under the framework document there should be a specific data privacy policy. It is important that management show the entire company that they understand and support the organization's privacy efforts. Evidence of support might include periodic meetings to focus on the topic, newsletter mentions that keep the topic top of mind, and/or signed/displayed statements of commitment.
1.5	Does the organization have a defined data security policy that is supported by the entire management team?	Under the framework document there should be a specific data security policy. It is important that management show the entire company that they understand and support the organization's efforts to secure their data and the network of computing resources that supports the organization. Evidence of support might include periodic meetings to focus on the topic, newsletter mentions that keep the topic top of mind, and/or signed/displayed statements of commitment.
1.6	If the organization includes union representatives, is there a defined process by which the union commits itself to support the data governance framework?	Unions are external groups that often represent a number of the organization's staff. Asking for union support of the data governance framework is an important part of the overall process of driving support across the entire organization's structure
1.7	Does the organization have a defined and documented definition of sensitive data or have they defined different categories of sensitive data so their employees are aware of situations where heightened care is appropriate?	Some data is more sensitive than other data and employees must be able to apply a level of behavior that is appropriate for the type of data they are using.
1.8	Does the organization have a specific individual that is responsible for data privacy and security matters?	An organization may have named the chief security officer, a chief data officer, a chief information officer responsible for privacy and data security or they may have specific duties to more than one individual. Regardless of how duties are assigned across the team, it is important that there be one

		identifiable person who is responsible for ensuring the organization publish, maintain, train, and support the organization's data policies and oversee procedures including dealing with questions, suggestions, complaints, etc. This individual would also be responsible for periodic audits that are designed to ensure compliance.
1.9	Is the chief privacy/security officer externally identifiable so that external parties (partners, customers, etc.) and authorities are able to quickly establish contact with that person's office via phone or email?	When an external party has a potentially important issue, they need to be able to identify and quickly contact appropriate resources. There should be multiple means to contact this person in the event that some contact methodologies are not functioning. Contact desks should be available 24x7.
1.10	Does the chief privacy/security officer have a senior management role and the authority to make and enforce organization wide policy changes?	Establishing and enforcing data privacy/security policies can cause conflicts with other organizational mandates and priorities. Ethical questions can also arise. The chief privacy/security officer should have a direct reporting relationship with the organization's senior most leaders to ensure privacy/security issues are properly prioritized within an organization.
1.11	If the chief privacy/security officer believes an issue is not being adequately addressed within the organization and its partners or if efforts to resolve an issue require heightened attention, is there a documented process to escalate such concerns?	The process for issue escalation should be well documented and there should be a process by which demonstrates the escalated issues are addressed in a timely manner.
1.12	Does the Chief privacy/security officer manage a sufficient budget and resources in order to implement the objectives outlined in the data governance framework?	Data privacy and security functions must be supported financially. There should be sufficient budget to maintain these systems and the policies outlined in the data governance framework. This includes maintenance of data inventories, and to conduct periodic audits. If there is insufficient budget to cover the functions of the framework document, the document should be descoped so management, customers, partners, and government authorities understand any limitations.
1.13	Does the chief privacy/security officer and all of their direct reports have a clear and documented mandate/charter that describes their specific responsibilities so there are not gaps or overlaps of authority related to minimizing the probability of an event (preventative), their responsibilities during an event (response), and their responsibilities after an event (recovery)?	The chief privacy/security officer and their team has the responsibility to reduce the potential for a negative event to happen, to respond appropriately when these situations arise, and then to recover after the fact. These responsibilities are often undertaken during a time of stress and the team can only work well if all rolls have been laid out ahead of time so there are no organizational issues during a time of crisis.
1.14	Does the chief privacy/security officer's office formally evaluate the risks of a process failure to personal data and the associated harm risks to data subjects so that purpose and use limitation can be appropriately considered?	The organization's privacy/security policies should be supported by deliberative consideration of the risks that manifest if the network is hacked or if untended data is removed from the company. Risks may be incurred to the organization itself, its customers, its partners, or other third parties. There should be documented evidence that these risks have been considered and steps that have been taken to minimize risks as well as actions that would be initiated if the risks materialize.
1.15	Does the data governance framework include an employee code of conduct that employees are expected to follow?	The data governance framework requires that all employees conduct themselves according to expectations that support the framework. Employees should be expected to commit themselves to supporting the framework and protecting the sensitive data within the organization
1.16	Does the chief privacy/security officer's office ensure that all new employees are trained in the data governance framework and its associated policies?	It is important that the new employees all understand the organization's data policy framework and how that policy relates to them as employees that might use or have access to data, as employees that interact regularly with customers, as employees that might interact with partners, or as employees that might use data to perform their job function.
1.17	Does the chief privacy/security officer's office ensure that all existing employees periodically undergo data policy training refresh exercises?	It is important the existing employees be reminded on policies and updated on policies changes associated with the organization's data policy framework and how that policy relates to them as employees that might use or have access to data, as employees that interact regularly with customers, as employees that might interact with partners, or as employees that might use data to perform their job function.

1.18	Are there defined and more intensive training procedures an employee must go through before they are granted access to sensitive data?	One way to increase data privacy/security is to ensure that people only have access to data they need to do their job and are denied access to extraneous data. There should be a formal process that allows people to apply for access to sensitive data and a formal process by which such requests are reviewed
1.19	There are many definitions of personal identifiable information. Does the organization have an organizational specific definition of personally identifiable information?	Personally identifiable information is information that can be used to identify a person when supplemented with external information. This is not a definitive definition because with enough external information, any data can be transformed into PII. It is important that an organization have its own definition that may include data about an individual, including an individual's first and last name (also maiden names), street address, email address, a telephone number, a Social Security number, credit-card/banking information, userid, passwords, or any other information that permits a specific individual to be contacted physically or online. The term often extends to include sensitive details such as a race/ethnicity, politics, relation, philosophies, trade union membership, genetic information, biometric access information, health, weight, marital status, sexual orientation, dependent or family information, person's birthday, employer, passport, patient ID, MAC or IMEI identifiers, vehicle or other asset identifiers, license numbers, photographs, education, height, weight or hair color that are collected in personally identifiable form. By having an official definition of personally identifiable information, the organization's employees will better understand the importance of making sure that data is treated properly.
1.20	Does the governance policy allow for differentiated data use cases? Is it clear that some data requires a higher level of vigilance than others?	The policy requirements often vary depending on whether the data is being used to support an operational process, a service, to market products/services, or to support research activities. Policies may also vary depending on the level of abstraction of the data in question, for example broadly generalized data often needs less scrutiny than data that relates to specific customers.
1.21	Do the organizations categorize the data used in its data use cases by its confidentiality impact level?	Impacts to the end-user (not to the organization) are higher if the data can be used to identify specific individuals, covers a large number of individuals, contains sensitive information (e.g. SSN), relates to a sensitive use issues (e.g. individuals with cancer), high levels of protection were offered to obtain consent, and the number of people with access to the data.
1.22	Has the organization created an operational environment where employees are aware of the data within the organization and that the employees are expected to properly care for and protect these corporate assets like any other corporate asset?	If the employees do not feel a sense of ownership and pride in the corporation's data privacy/security policies, they will often neglect to give these policies the attention they warrant.
1.23	Does the organization have enforcement rules to ensure employee compliance with privacy/security policies?	The only way to ensure compliance with established data policies is to periodically conduct an audit to make sure the policies are being adhered to and so that identified issues can be corrected.
1.24	Does the chief privacy/security officer's office ensure that all new partners are trained in the data governance framework and its associated policies?	It is important that the new partners all understand the organization's data policy framework and how that policy relates to them as partners that might use or have access to data, as partners that interact with their customers based on the organization's data, or as partners that might use data to perform their job function.
1.25	Does the chief privacy/security officer's office ensure that all existing partners periodically undergo data policy training refresh exercises?	It is important the existing partners be reminded on policies and updated on policies changes associated with the organization's data policy framework and how that policy relates to them as partners that might use or have access to the data the organization is responsible for, as partners that might interact with their customers based on the organization's data, or as partners that might use data to perform their job function.
1.26	Does the chief privacy/security officer's office have a process to formally notify the organization's management of any changes in legal requirements that might impact	Each change in the legal requirements should initiate an evaluation of whether the data protection framework should be changed. These legal changes could change management responsibilities and may require change notices

	some aspect of the data governance framework?	to be sent to customers and/or partners, changes to the website, and possibly changes to the posted policies/procedures.
1.27	Does the chief privacy/security officer's office ensure that all new employees have formally agreed to the employee code of conduct that includes data governance issues?	It is important the new employees formally commit to supporting the organization's data policy framework so there is a clear record that every employee is trained and aware of these policies.
1.28	Does the organization treat their privacy policy as a customer commitment? Does the organization have a process by which they discuss or otherwise communicate their commitment to data privacy and security with their customers?	Privacy and security policies should be treated as an agreement between organizations and their customers/partners. While these issues are often treated as a legal issue, these issues often go beyond that to impact the image of the company in the market.
1.29	Is it clear how an employee, customer, or partner would contact the chief privacy/security officer's office for any issue related to processing or management of the data the organization is responsible for?	Protection of data requires the participation of the entire organization (including customers and partners). It is important that everyone have a well-defined path to ask questions, raise issues, or exercise their rights with respect to data privacy and security
1.30	Does the organization have a monitoring process to ensure that copyrighted or other improver material is not posted to the internet or shared with partners/customers without proper permission?	A company's assets would include data that have been copyrighted and is protected by another source. Copyrighted material is normally thought of as photographs, songs, book content, and movies but data can be copyrighted as well and this data should be appropriately tagged as such.
1.31	Does the organization have a process by which people can complain about inaccurate or copyrighted content and ask that content be removed even if the data does not pertain to them?	Accidently, protected data may be submitted and maintained in the organization's data asset base. Organizations should have a method to document properly approved work that they host so that when a complaint is raised, the provenance of the data can be investigated so appraisal action can be taken.
1.32	Does the chief privacy/security officer's office maintain a list of relevant government agencies, local and non-local that may need to be contacted in the case of a data event? Are the conditions that warrant notification and the processes for notification well defined?	Data networks do not respect geopolitical boundaries. Different government entities require different reports on malicious or accidental data issues. It is the responsibility of the chief privacy/security officer's office to report issues of concern to the proper government agencies even if the organization is outside the jurisdiction of a specific organization. For example, many government agencies want to be notified of a data breach that occurs in a different geographic region if the breach affects their citizens.
1.33	Does the incident file clearly identify the relevant government authorities that have been notified or that may need to be notified?	The impacted data will need to be geo-tagged as to where it was collected, stored, processed, and what geographies it traversed. If it is not, it may not be clear where notifications should be sent in reaction to a breach event. All data should be geotagged as to where it was generated and the source of the data ownership so incidents can be properly managed.
1.34	Does the organization advertise a privacy or security position to customers, partners or shareholders?	If the organization advertises a specific position, the organization can be held to that standard even if the advertised message is not in line with the stated privacy/security policies of the organization
1.35	Would an external privacy/security practitioner describe the organization's measure of data security as reasonable?	The definition of reasonable is intended to imply an industry standard which will change over time. Therefore there is an expectation that the organization will keep up with industry norms with respect to data transmission and data storage security standards
1.36	Does the organization advertise an affiliation with an industry association that has established privacy/security standards?	Advertising membership in an industry association may present the appearance that the organization subscribes to the privacy/security standards the association has established for its members.
1.37	Does the data privacy/security policy define special classes of individuals which require unique types of support?	As an example, if individuals are identified as members of a labor union, if they have criminal record (or convictions for specific crimes), if they are government officials (such as police or emergency response teams), subject to an ongoing government investigation, or other special circumstances, special privacy rules may apply to management of these records
1.38	Does the data policy describe how/when it is permissible to use data to target advertisements or other messages to individuals?	An organization might have policies that only allow specific kinds of data for targeting messages to individuals. They might also have policies that limit such message delivery to specific times.
1.39	Are employees and partners directed to NOT keep unauthorized or duplicate copies	Employees in need of data or other records should be directed to access the central data repository of data, use that

	of sensitive data on their local computer, personal electronic devices, off-line storage, or in paper form.	information, save it to the central storage if changes have been made, and to eliminate any local copies.
1.40	Is the organization registered within the state to buy or sell data?	Some states require that companies which either buy or sell data register with the State as participating as a data brokerage
1.41	Does the organization have an organization wide privacy policy AND a series of project specific privacy policies that details how that project is permitted to use data?	Organizations should not attempt to construct one general privacy policy that covers all projects with generalized statements but should instead have a master policy complimented by detailed, project specific descriptions of how data will be collected and used by individual projects

DATA AND PROCESSING INVENTORIES

For an organization to audit their privacy and security framework, they have to keep an active inventory of the data their organization directly or indirectly is responsible for managing. They also need an inventory of all the processing functions (software) that manipulates or generates new data based on existing data content. The organization cannot conduct a reasonable audit if it is unaware or these systems are not visible to the audit team

2.1	Is there an accurate list of all physical locations where data is stored that can be quickly accessed and does that inventory identify what specific data is located in which location?	Periodic audits should be standard practice and this can only be done if there is a clear inventory of where the data controlled by an organization can be found. A central directory (inventory) of all data storage centers also simplifies post-breach forensics and makes it easier to deal with potential government interventions.
2.2	Does the organization have rules that indicate what kinds of data collection and storage is expressly prohibited?	Organizations will often collect and use data for specific functions and discard the data once the process has been completed. If the data is immediately discarded, it is reasonable to also inform the individuals about discard policy when initially obtaining the needed data.
2.3	Does the organization have a defined data retention policy that defines when specific data and records are to be deleted as a part of their data governance framework?	Retention policies establish standards for the retention and deletion of records. The fewer sensitive data records an organization maintains, the less potential there is for data to be compromised. Many laws also specific minimum data retention periods that must also be met. All records should be time stamped with their creation date to make it easy to identify data that has expired (and should be purged).
2.4	Does each inventoried data set specify if the data MUST be kept until a specific date? Does it also specify a specific date when the data should be deleted?	Data has expiration dates by which it should be deleted and the date should be shared with those described in the data set. Also, data must be kept by a specific date to make sure there was a record of how the data was used.
2.5	Does the organization document when/how data is transferred between sites for storage and processing?	Many laws put restrictions on data that is passed across geopolitical borders. When data moves across a border, it often implies that the laws of both countries are requirements that the organization must meet and this makes management of the data more difficult. It is often safest to keep data in the region where it was generated. Regardless, transfers of data to another area or across an intermediate area should be documented
2.6	When data is transferred to another organization or across geopolitical boundaries, is there documented evidence that the receiving supervisory authority accepts the policies and safeguards requested by the transferring organization?	When data is transferred between companies or divisions within a company, a contractual agreement is often necessary to demonstrate the data was transferred under the enforceable expectation that privacy/security process would not be disrupted.
2.7	Is there an inventory of all data processes (applications) that are hosted within the organization, used by partners, or operating in a cloud environment with a description of what that process does?	Periodic audits require a clear inventory of where the data controlled by an organization is being used or manipulated. A central directory (inventory) of all data processing centers with a description of the applications hosted at those centers also simplifies post-breach forensics and makes it easier to deal with potential government interventions.
2.8	Does the organization have rules that indicate what kinds of data processing is expressly prohibited?	As a preventative measure, some organizations will expressly forbid certain types of data processing and data collection practices. If data is collected for a permitted use, it is reasonable to also inform the individuals about data prohibitions when seeking permission to use the data the data
2.9	Does the organization have documented privacy/security policies that require disclosure to data subjects when it begins to collect new types of personal data?	When a new data process is started it may involve collecting new data from data subjects and the organization needs to disclose the nature of the program to the impacted individuals. If the new program reuses existing data, the new processes were likely not included in the disclosure statement made when the data was collected so these individuals need to be contacted and informed about the new use case.
2.10	Does the inventory process seek to identify virtual assets that may exist on a temporary basis, what they are used for, and where these virtual assets exist?	As the industry moves to virtual assets, it becomes important to maintain an inventory of these 'possible' assets that may be spawned and then killed as these processes represent potential data processing stations that the organization is responsible for.

2.11	If cloud processing is used, is it possible to determine where the data is processed and the geographies the data might traverse as it enters and exits those cloud based processors?	Many governments and organizations have specific geographic prohibitions about where data is processed. Some restrictions even come into play if the data traverses a specific geography as it flows to or from a cloud based application (including edge based virtual environments). To demonstrate compliance with such requirements, the organization will have to be able to show that they understand how/where their data is being processed by internal and external cloud systems.
2.12	If data is stored in the cloud, is it possible to determine where the data is stored and the geographies the data might traverse as it enters and exits those cloud based storage systems?	Many governments and organizations have specific geographic prohibitions about where data is stored. Some restrictions even come into play if the data traverses a specific geography as it flows to or from a cloud based storage system (including edge based virtual environments). To demonstrate compliance with such requirements, the organization will have to be able to show that they understand how/where their data is being held by internal and external cloud systems.
2.13	Does the inventory of all computer equipment include laptops, servers, desk-side, and other hardware, software by release level (operation system and application)?	Inventory scans should be done periodically to watch for equipment installations that have not been approved or for software that is not being updated on a periodic basis
2.14	Is there a data inventory that describes the location and type of all IoT (Internet-of-Things) devices that are generating data?	IOT devices can generate large amounts of data and the organization is responsible for that data. This makes it important that the organization be aware of the location of all IOT devices and the nature of the data that the device generates.
2.15	Does the inventory of all communications equipment include hardware, software by release level (operation system and application)?	Inventory scans should be done periodically for all routers, hubs and other communications equipment to watch for equipment installations that have not been approved or for software that is not being updated on a periodic basis
2.16	Does the inventory of mobile equipment including smartphones, tablets, and other hardware, software by release level (operation system and application)?	Inventory scans should be done periodically to watch for equipment installations that have not been approved or for software that is not being updated on a periodic basis
2.17	Data that has been copied and stored or used on personal machines is difficult to protect and audit. When employees or partners download data, is there a procedure where they have to 'check-out' the data and is there a process by which they indicate they have deleted or otherwise moved the data off their personal devices?	If a copy of protected data is copied and used outside the purview of the central staff, the organization still remains responsible for ensuring the protection and security of that data. This makes it important for an organization to know who has taken copies of such data and where these copies exist.
2.18	Does the organization have to track usage of protected and sensitive data assets and periodically report usage statistics?	Some licensed data content base licensing fees (royalty fees) to unfettered use of the data while other licensed content base licensing fees on usage. A system for tracking and paying licensing fees based on data usage should be supported
2.19	Does the organization segment Personally Identifiable Information from the data and store it in an encrypted file (using pointers to link the two files)?	By segmenting the data into linked data sets, if one data set is compromised the data from the other data set can be safe. This allows the organization to allow employee access to the data without allowing them access to identifying information.

DATA MANAGEMENT

The organization's Data Policy is an important part of the data governance framework. It describes the behaviors expected from an organization's employees with respect to privacy and data security. Sections of the policy should also describe the privacy policy with respect to employee data. While this employee data policy is for the organization's internal use, the public data policy should be readily available to the public. Either or both policies can and should be shared with partners and other organizations which are expected to uphold and support the relevant organization's policies.

3.1	Does the organization maintain a log that details which data processes have been executed, when they were executed, where they were executed, and the data that was used by the process?	Regardless of the existence of a consent agreement that might describe multiple permitted uses of the data, there should be an active log that describes which processes actually made use of the data in question. A consent agreement provides permission but does not obligate an organization to process the data as described.
3.2	Does the organization maintain a list of other organizations that have access or visibility to the information collected or held by the organization?	In the case of a breach or other data management issue, it is important to be able to reach out to these other organizations. In addition, if a data breach is reported by another organization, it will be important to be able to quickly ascertain whether your organization might be impacted.
3.3	Does the data management policy call for deactivation of internet links to organizations that violate laws, intellectual property rights, or the organizations internal data policy?	Pointing users to sites with objectionable business practices will make the organization a participant in the process of driving users to those sites. When the organization's data assets point users to sites with data policies that the organization does not support, they are in effect encouraging individuals to visit sites that might be harmful.
3.4	Does the organization code data so identifying information is stored in segregated files and encrypted separately from data used by other processes.	Data processing often does not require identifying information to conduct statistical analysis of data sets. By separating the identifying information from personal data and managing them independently with different passwords and different need-to-know criteria, data security levels can be increased.
3.5	Does the organization anonymize data at the earliest possible moment and are the anonymization algorithms tested to ensure the identity of data subjects cannot be identified?	Anonymized data is less of a risk that personally identifiable data. Anonymized data is still sensitive because it can be linked with other data to triangulate on a specific individual. Anonymized data should be tested to make sure identifies cannot be uncovered from masked data
3.6	Does the organization release anonymized data to third parties?	It is possible that anonymized or statistical data may be released without consent, however, if a third party can combine the data with other data to uncover the identity of an individual, the organization could be held at fault.
3.7	Does the data policy state the conditions under which data will be released to specific government authorities?	Many organization's data policy demand a warrant or other court order before the organization will give electronic data to government agencies, but regardless, the organization should be clear about the level of privacy the employee has while at the organization of at home when remotely connected to organization by a network
3.8	Does the organization have documented procedures that define the periodic reports that must be sent to appropriate government authorities? Is the contact information for these authorities well documented and are report submittals well documented?	Many government agencies expect periodic reports on data breaches or the lack of a data breach. The organization should have a list of such requirements and they should have a person identified as the party responsible for the timely filing of such reports.
3.9	Does the organization have documented procedures that define when periodic reports are to be sent to the appropriate management representatives within the organization? Is the contact information for these authorities documented?	Management of the organization should be made aware of any data breaches as well as any open issues being addressed by the office of the data privacy/security officer so they have the opportunity to intervene if there are issues that need increased attention.
3.10	Does the organization periodically audit their data policies to ensure that data is only being used for documented purposes and not being used for other purposes?	There should be a well-defined log that describes what data has come into an organization and how that data was used. Periodically, these logs should be checked against the organization's data privacy/security policy and against the consent agreements to ensure the processes are being followed and that the data is not being used for undocumented purposes.
3.11	Does the organization undertake a risk assessment before initiating a program that	The organization's risk assessment process should not be driven by a member of the team that will benefit from the

	collects or processes data in order to determine the potential harm that might ensue from a breach?	collection process; instead, the process should be conducted by an independent party who is able to consider the risk potential from the data subject's point of view.
3.12	Does the organization's risk assessment process consider the potential harm that might come from a) unauthorized access to the data by the organization's internal employees or b) accidental destruction or alteration of personal data?	Data breaches and other security errors often come from accidental actions of the organization's employees. While the root may be intentional, they are often the result of an unintended action
3.13	Are the data policies posted in an easy to find location for employees, customers, and partners?	Privacy policies should not be difficult to locate or review. When policies are posted but in hard to find locations, the situation makes if hard for employees to refer to this material, often at times when the employee is in need of guidance
3.14	Does the organization maintain a log of requests to copy or transfer some portion of the data in a data set?	If the data is given to a third party, the log should record the name and contact details for the receiving party as well as their data protection officer, the purpose for the transfer of the data (including a list of limits or prohibitions against processing the data), and a description of the transferred data. Many data privacy rules apply across geographies making it important to know where data resides, where copies may be located, and whether the transfer may be across a geopolitical border.
3.15	Does the organization maintain a log of requests to access data in a data set?	If the data is accessed, a log should be kept that reflects who accessed the data, the purpose for the access, and a description of the specific data accessed. Should the data be breached, it should be easy to forensically identify how the organization should respond to the breach.
3.16	Does the organization maintain a log of requests to modify data in a data set?	The register provides a definitive record of what data has been processed and is needed to demonstrate a proper chain of custody. The log for a change request should show the source of the request, the original data, and the resulting disposition of the data.
3.17	Does the organization maintain a log of all requests to add or delete records in an active data set?	Record creation or deletion requests should detail the source of any create or delete activities as well as the reason for the addition or deletion. For example, was the data deleted by request of the consumer, has it exceeded time limits for holding data, was it found to be in error and purged, etc. ?
3.18	Does data deletion processes overwrite deleted data with zeros so the data cannot be recovered?	When data is deleted from a computer, the references to the data are typically erased but the data often remains in storage and can potentially be recovered. To ensure the data to be erased from a computer, it is best to write over the existing data with garbage data before the data is deleted.
3.19	Can the organization provide activity reports for individual data subjects or per incident that describe a) any transmitted personal data-breach notifications, b) corrections of personal data or data deletions, c) summary identification of the data associated with the individual held by the organization (or a third party), d) descriptions of why and how the data was collected, and e) any data transfers to a third party?	A periodic activity log that describes how the data held by an organization has been used as well as activities that have been undertaken to maintain the data serves to keep individuals that the organization has a data consent relationship with and serves to ensure an ongoing dialog with the individual.
3.20	Does the organization make it clear that when it discloses information externally for statistical and other reports, that specific identities will be masked unless otherwise noted?	Information about employees, shareholders, officers, etc. may need to be disclosed in order to sell, buy, merge, or otherwise manage the business. Data may also need to be released to resolve labor or other legal disputes. When data that identifies individuals is released, it should be made clear the circumstances when this will be done so individuals are not caught unaware.
3.21	When others post content to an organization's website site, is the content either a) properly attributed to a validated source or b) or is the content validated so the organization assumes responsibility as the creator?	An organization is responsible for content posted to their web site by users unless the organization attributes the posting to someone else. When attributing postings to an external entity, the entity should be validated and traceable back to its source.
3.22	If Artificial Intelligent systems are used, are processes in place to make sure the AI engines do not violate the procedures and processes laid out in the data governance framework?	Data governance policies are usually written with the assumption that the organization's personnel will follow these policies. When automation is introduced into operational processes, the rules that drive such automation have to be checked to make sure the machine directed actions do not

		ever result in violation of the organization's data governance policies.
3.23	Do the rules about handling of data apply equally to digital data and paper data (re. data handling, recording, disclosure, and storing, correcting, deletion)?	Whether data is stored electronically on disk or in a paper report, the same rules should apply to all personal-private data.
3.24	Paper records may contain sensitive personal information. Do the data governance policies require that paper records be physically secured and shredded/burned when they are no longer needed?	Where personal data processing involves any steps in countries outside the European Union (EU), governance provisions are defined and implemented to ensure that organizational data protection and privacy arrangements are maintained and enforced regardless of jurisdiction.
3.25	Does the organization flag publicly available information as being distinct from private information? Does it capture the source that validates the public publication of the data?	Publicly available information such as information in public records (court documents, publicly published, included in a directories), are often treated differently from private information.
3.26	Does the organization have the means to use log files to recover data changes that occurred after the last backup?	In the case of a catastrophic failure, systems can be recovered from backup files, however, changes made to the system after the last backup can be lost but these changes should be recoverable from the system log files.
3.27	Does the organization have a process that requires that the generated IOT data has an expiration date forcing the data to be deleted after a defined period of time?	IOT data should not be treated as a permanent data but should be treated as a digital twin of the physical world that will be deleted once the data is no longer of value.
3.28	Are database systems encrypted and properly secured to prevent unauthorized users from accessing the system?	Access to a database system should be secured to ensure only authorized users have access and the data should be encrypted. Also, a secured database system should never be used to support/allow access to unsecured data. Unsecured databases should be independent from secured databases.

PRIVACY POLICY

The Privacy Policy is publicly visible document that describes the organization's commitment to maintaining the security of their information processing systems and their commitment to ensuring the privacy of their customers is maintained

4.1	Does the organization's privacy policy include a single public facing statement of principles that covers the entirety of the organization? The privacy policy should be legally explicit and also clearly stated so it may be understood by an average person.	Privacy policies should not be difficult for external parties to locate, review, and understand
4.2	Does the organization have multiple privacy policies that cover different divisions or groups within the same organization? If so, does the policy indicate the situations where the policy applies and the specific situations where it does not?	When an organization has multiple privacy policies, users may not understand when which policies apply. This has to be made clear so it does not appear the multiple policies are an attempt at obscuration.
4.3	Does the organization make use of different forms of consent depending on the type of data collected or the data processing projects (in contrast to using a generic form with little program specifics)?	The privacy policy is an organization wide agreement whereas a consent agreement is program specific. The consent agreements should describe a list of collected data and a list of potential uses for the collected data. If the consent agreement covers different kinds of data or different applications of the data, the individual should be able to accept some consent agreements and to reject others.
4.4	Does the organization post its privacy policy on the internet so it is easy to find from the organization's home page?	Privacy policies should be posted on the internet, dated, and available either on-line or in printed form
4.5	Does the organization's privacy policy indicate the policy effective date?	If the organization holds data that is covered by an older, non-current data policy, the organization should post the current and the older policies. They should also describe when the older policies apply and when the newer policy applies.
4.6	Does the organization's privacy policy describe the handling of the information it collects about individuals that visit its web site?	The privacy policy should identify the information collected from web site visitors and describe how data will be used and protected within the organization. The organization does not need to ask users for their consent before they are allowed to browse the web site, but this should be done before any information is transmitted from the user's device to servers the organization controls.
4.7	Does the organization's web site make it clear what data is collected from web site visitors and describe how this data will be used?	Users should be notified what information is collected and tracked about people who visit their web site and how that information is being used by the organization.
4.8	Does the organization's privacy policy identify the information it collects about people that use open online services?	Many organizations have public and controlled data on their web pages. If the organization collects behavioral data about anonymous users to their public sites, an explicit consent agreement may not be needed, however, the organizations posted data privacy policy should clearly identify the information that will be collected from these individuals and describe how that data will be used.
4.9	Does the organization's privacy policy describe the organization's policy related to cookies?	Cookies and similar technology can be used to remember a customer's last visit to the organization's web site so the interactions with the customer are a continuation of prior interactions. If the cookies transmit any data from the visitor's device to a server under the control of the organization, permission should be obtained before the transfer is allowed to happen.
4.10	If the organization installs and uses cookies, is this practice disclosed to the web site visitors and are they told why cookies are important to the process? Are users given the option to refuse the acceptance of cookies?	Users should be notified what information is tracked by any cookies and how that information is being used by the organization.
4.11	Does the organization have a process that allows individuals to remove the posts they have made to the site?	Individuals should be able to delete/remove any posts or data submissions they have posted to an organization internet web site.

4.12	Does the organization disclose how they respond to customer "do-not-track" requests?	Some web browsers have do-not-track preferences which cause a do-not-track message to be sent to visited websites, however, not all websites treat these messages equally. The organization should explicitly state whether the website recognizes these messages and how they respond to such requests.
4.13	Does the organization have a process that allows minors or their guardians to remove the posts the minor has made to an organization's site?	Minors and their guardians should be able to delete/remove any posts or data submissions that may have been made to the organizations website
4.14	Does the organization's data privacy policy prohibit monitoring any electronic communications (e.g. email, telephones, ..) between two parties unless both parties consent?	Employees expect privacy in their telephone conversations and these expectations could be extended to include email and other electronic forms of interaction. Organizations should be clear about what employee behaviors are monitored and should consider the expectation of the other party the employee might be communicating with.
4.15	Does the organization ask employees to consent to possible electronic monitoring of communications as one of the terms of employment?	Companies can monitor telephone calls and emails of their employees, however, these communications could be considered a private exchange between two people. If a company occasionally monitors the employee's email or phone conversations, would it become important if the employees are made aware of these policies?
4.16	Does the organization's privacy policy describe what the organization does in response to a do-not-track request?	If an individual asks that their activities not be tracked when the user accesses their open website pages, does the organization honor that request. If the user is detected using tracking blockers and other anonymization technologies, the organization may refuse to give the user access to some content but they should be prohibited from surreptitiously collecting the information.
4.17	Does the data policy require consent of the portrayed people before posting and distributing images of the portrayed people?	Posting of video, pictures, or other likenesses often have special requirements attached to them. Some such content is covered by copyright law but even for non-copyrighted material special rules may apply depending on whether the individual is in the public eye or not. Whenever images are considered for posting, the images should be considered private until the image has been approved for public posting.
4.18	Does the organization have a privacy policy for data collected from data collected from license plate readers?	License plate reader systems were developed to help manage parking garages. License plate numbers may not in itself be considered sensitive information but it is easy to combine that with vehicle registration information and that makes it sensitive data. In doing so data from these systems can be used for other purposes that may be considered invasive.
4.19	Does the organization have a privacy policy for data collected from connected televisions?	Smart televisions generate data related to the consumers viewing habits. More advanced televisions are able to monitor the room for sound and can take pictures as well. If smart televisions are used within the organization or if data is collected from television based systems, the organization should be clear about the data collection and use of this data.
4.20	If the organization makes any use of drones, does the organization's privacy policy describe the process for obtaining the permissions needed to fly over private property?	If the organization operates a drone and it travels over private property without permission of the property owner for the purposes of capturing images or sound, the organization could be liable for privacy invasion unless consent has been established ahead of time.
4.21	Does the organization's policies allow people to request a copy of all the data held by the organization?	When a person requests that an organization provide them with a description of the data that relates to them as an individual, the organization should have the ability to create a report in a format that the consumer can understand, and deliver the report for free (or a reasonable administrative fee) in a timely manner.
4.22	Does the privacy policy describe how the organization will notify people about changes to its privacy policy?	Privacy policies do change. If an individual has given permission to an organization to use their data under an old privacy policy, the individual should be told about the new data policy. This also applies of historic data is held about an individual and the policy changes, the organization should still explain the new policy even though the organization does not have an ongoing relationship with the individual
4.23	Does the organization have records related to an individual's interactions with the legal system including both civil and criminal interactions within the local and a remote jurisdiction?	Legal interactions may or may not be considered personal information. Often the determination rests in whether the interactions are publically accessible

4.24	Is there a documented policy that calls for the periodic validation of personal data to make sure it is accurate and up to date?	When an organization undertakes a program to collect data, it becomes the organization's responsibility to make sure the data is accurate. This means the data needs to be periodically validated to make sure it is still accurate.
4.25	Does the organization's data governance policy require the organization obtain the explicit consent of an individual before collecting, using, or disclosing the customer's personal information?	The organization should have a started policy that direct employees not to start any data collection program until the individuals affected by the policy have explicitly consented to participating in the program
4.26	For each data collection program, is it clear where the data consent and other records associated with that data collection process can be found?	Collecting data consent agreements and requests to edit data or change permission grants should be documented and easily accessible for future reference
4.27	Cross-border data flow laws may preclude certain transfers, prevent specific data collection processes, or even require notification of specific authorities based on the citizenship of the data subjects. Is the citizenship of each subject documented, are the permissible data activities moderated based on citizenship and are there auditing procedures to make sure compliance is achieved?	Most data laws are written to apply to data in a country or data that relates to a country's citizens. This makes it important that all user specific data identify the citizenship of each data subject so the organization will understand the data collection laws that apply to that specific individual.
4.28	There are sensitive situations when a user's consent is not required to collect data, are these consent exceptions well defined, easy to understand, and well documented in the privacy policy?	For situations where research is intended for the public good, individual consent agreements may not be necessary. For example, British Columbia allows use of personal information in health research without consent as long as the research is in the public interest. Research that is being conducted for the public good may have specific requirements associated with it and these requirements should be documented and evaluated for compliance before any such research is undertaken.
4.29	When a user requested action implies consent, does the policy stipulate that consent is required to complete the action?	A separate consent agreement is not needed for situations where a requested activity implies consent but the organization should make it clear what data will be collected from the individual and from third parties and how that data will be used (and protected). For example, implied consent is possible when the individual has an interest in a pension plan and the pension plan needs to use the individual's personal information to create an account or to provide coverage under the plan.
4.30	Does the organization policy make it clear when information about the organization may need to be disclosed as a part of a business transaction?	Information about customers, employees, shareholders, officers, etc. may need to be disclosed in order to sell, buy, and merge stock or to transact business.
4.31	Does the organization have device policies that ensure the network infrastructure will not be compromised by the installation of computing/IoT devices that can be secured?	A data security policy can only be implemented in a network where the devices that make up the network are able to support the policy. There are many recommendations that describe the features that a securable device should support. The organization should have a device acceptance policy that only permits devices with the features needed to support its data security policy to access the network resources
4.32	Does the organization have a policy in place to detect and protect against devices that have been connected to the network infrastructure that do NOT meet its security standards	Even if the organization has a policy in place prohibiting unsecured devices from being connected to the network infrastructure, it should be expected that people will knowingly or unknowingly connect unsecured devices to the network. These situations must be detected and protected against
4.33	If the organization sells or resells hardware or software, has the organization verified the product provides a reasonable set of security features	Some laws have made anyone that sells a product without security features liable if the lack of security in a product results in a breach. The definition of reasonable includes (but not limited to) the use of a device specific password (not a vendor generic password), the ability to track individual data connections, the ability to perform software updates, the ability to change security settings, and the ability to deactivate network access points.
4.34	Does the organization's privacy policy prevent disclosure of goods and services purchased or used?	Specific laws prevent libraries from disclosing book borrowing data but in general this is a good principle. Disclosure of individual activity data should be avoided if possible.
4.35	Does the organization's policies prohibit false representation online?	The company misrepresents themselves or misrepresents others on line or in any electronic exchanges. Any references to external parties should not be permitted until documented permission from the other party is obtained.

4.36	Has the information that local laws saw must be physically posted at an organization's buildings also been posted on line?	Many laws define specific physical signage requirements that must be posted for employees, customers, and patients to see. This same information should also be available on the organization's website.
4.37	Has the information that local laws saw must be given to customers, employees, and patients also been posted online?	Many laws define specific physical handouts that must be given to employees, customers, and patients. This same information should also be available on the organization's website.
4.38	Has the organization posted descriptions of situations that might force the organization to file a report with an external organization?	Many local laws indicate that under certain conditions, information reports must be filed with various government agencies. The web site should make people aware of the conditions that might require an organization to file a report with an external organization.
4.39	Has the information contained on the web-site, including privacy and security policies, been tested to ensure that it is properly translated to other languages via language translators?	Many web browsers are capable of auto-translating web site content from one language to another but these translations may not always be accurate so it is important to test the translation process before suggesting their use.
4.40	Are forms, documents, and other web-site content available in other languages?	Not everyone who needs to know about an organization's policies is fluent in English and efforts should be undertaken to ensure everyone is capable of understanding important information.
4.41	Does the organization's systems provide a mechanism so that those that access an organization's policy document have the capability of electronically acknowledging they have received and understand the policy.	People accessing electronic policy statements should have the ability to electronically acknowledge their acceptance and understanding or to withdraw an acknowledgement they may have made at an earlier time/date.

THIRD PARTIES

In today's interconnected world, organizations connect with other organizations; they work together as partners, customers, and suppliers. Inappropriate actions of any of an organizations related third parties can damage the organizations reputations. This makes it important to manage any organizational relationships connected by data just as the organization manages its

5.1	Does the organization have a list of all partners that the organization shares data with including contact information of key personnel?	For each partner (or subcontractor) that the company provides data to, the organization should have primary and secondary contacts (name, title, address, email and phone) so these people can be quickly contacted in the case of an emergency. The entries in this contact list should be verified for all active and inactive partners.
5.2	Does the organization do annual reviews of the data policies for all active partners to ensure the partner's data policies meet the organization's expectations?	For each partner (or subcontractor) that the company provides data to, the organization should review the partner's data policies to ensure the partner's data policies meet the data governance policies of the organization.
5.3	Above and beyond an exchange of data policy information, when data is given to a third party, is there an explicit agreement that spells out the nature of the data that has been provided, the purpose for the exchange, when the data is to be deleted or returned, notification and periodic reporting requirements, as well as any explicit requirements that must be met to safeguard the data?	Data policy information generally relates to overall organizational data policies, however, additional information must be exchanged to describe specific data exchanges so both organizations understand not just the policies, but the data that each organization has and its intended use (and restrictions)
5.4	When an organization establishes a relationship with a third party, does a part of the formal process require both organizations to review the data policies of the other third party?	When data is provided to a third party, the original organization is still responsible for ensuring the third party properly cares for and manages the data. When an organization establishes a relationship with another party, both data policies need to be considered to ensure the other party will not become a weak link. These policies and procedures must also be periodically audited to ensure the needed protections are in place and operating as expected.
5.5	Are all third parties that send data to the organization or receive data from the organization required to notify the organization of any changes in their data policy with the understanding that such changes may nullify established business relationships?	Data policy needs to be exchanged and considered at the onset of a business relationship between two organizations. However, data policies do change over time and if either organization changes its data policies, notices must flow to partnered organizations so that they can consider whether they are accepting of the policy changes or if they believe the changes require a re-negotiation of the organizational relationship.
5.6	For any established relationships with a third party, the organization should periodically audit the other party's data protection operations to ensure the policies are operating as expected.	When a third party relationship is established, the original organization cannot assume the receiving organization's data processes are operating properly based on the existence of a data policy. Policies must be audited and detected shortcomings must be overcome. The originating party is responsible for ensuring the third party properly care for and manages the data.
5.7	If the organization has an agreement with a third party for use of specific data for a specific purpose and the organization suspects the other party is violating that agreement, is there a defined process to request corrective action with the potential to terminate the relationship if the corrective actions are not satisfactory?	When two organizations have a relationship that allows the transfer of data, the source organizations should have a process to check that their data policies are being adequately supported by the partnered organization. If issues are discovered, the source organization should be able to request corrective action and to terminate the relationship if the requests are not satisfactorily addressed.
5.8	When data is transferred to a third party, is there documented evidence that the receiving party has agreed to apply the originating organizations privacy and security policies to the received data?	If the organization has data that is covered by its privacy policy and transfers the data to a third party, the transferring party accepts the obligation to verify the receiving organization is maintaining the data in accord with the original data policy. The log of such data transfers should identify the receiving party and the data protection officer that has accepted responsibility for safeguarding the data.
5.9	Are data-policy checks built into the purchasing process so the organization's approved vendors have been examined to	When two organizations have a formal business relationship, data flows between the organizations and each organization needs to accept and support the other organization's data

	ensure their data-policies meet with the approval of the organization before they are accepted as an approved vendor?	policies. Sometimes the data that flows between the organizations may be transferred data files, sometimes it might be in the form of correspondence, sometimes it relates to business operational data. All data has the potential to require agreed levels of care and maintenance.
5.10	Are data-policy checks built into the sales process so the organization's customers do not receive data if their data policies have not been examined to ensure their data-policies meet with the approval of the organization?	An organization's customers should be treated as partnered organizations because data about business transactions flow between customer and the organization even if digital files are not directly transferred.
5.11	When an organization provides data to one of its partnered organizations, is the partner required to confirm receipt of the data and acceptance of the policies that the third party expects so that the source organization maintains visibility of the data supply chain?	Once two organizations accept each other's data policies and have determined there is specific need to exchange data for a defined use, when the organization physically sends data to a partner, they should expect the other organization acknowledge receipt of the data and an indication that the required data policies are understood, forensic and notification efforts become much easier.
5.12	When the organization receives data from a third party, is this data logged as to its source (including company name and the name of the data protection officer) as well as any data protection requirements that are associated with the data?	When an organization receives data from a third party, they are also accepting the responsibility to protect the data in a way that meets the expectations of the transmitting organization.
5.13	When data is received from a third party and it is associated with data policies of a source organization that is not part of the organization's data policy, are these requirements checked to make sure your organization can accept data with these needs?	When data is received from a third party, the source organization may attach care and management that your organization is not able to commit to. The data requirements need to be initially examined and committed to before the data can be accepted.
5.14	Explicit consent may not be needed if the data is needed to fulfill the contract with the data subject, if it is needed to protect health and wellbeing of the data subject, or if it does do not infringe upon the data subject's rights, however, for situations where consent is not required, the situations and the justification for not requesting consent should be well documented in the privacy policy.	Consider the case where the police maintain a record of criminal histories, this data can be compiled and used without the data subject's consent but it should be well documented why consent is not required in such cases. Additionally, publically available data does not need explicit permission to be tracked as the data is already available for public observation.
5.15	For a specific user, can the organization generate a list of all consent agreements the user has accepted or denied?	While an organization might have one data security/privacy policy, they should have individual consent agreements for each data collection program that an individual user participates in. The organization's administrator should be able to generate the list of each consent agreement associated with each user.
5.16	In the event that data is held by a third party (a data custodian), if a third party seeks unauthorized access to the data, will the custodian report the data is locked and refer the inquiring party to the responsible organization for permission?	When an unauthorized party seeks to access data that is being held by an organization's partner, the partner should refuse access, direct the requesting third party to the organization, and report the request to the organization.
5.17	If necessary, does the data policy make it clear that if the organization may need to exchange data with a third party in order to complete a financial transaction, the third party will be required to delete the information when the transaction has been completed?	Transactions are special use cases in that an exchange of sensitive data is needed to complete the transaction. If the transaction does not complete, all sensitive data must be immediately destroyed. If the transaction completes, the data can be saved as part of the transaction record as long as it is properly secured.
5.18	If IOT data is obtained from a third party, is the third party made aware of when the IOT data they have provided will be deleted?	IOT data from a third party has a shelf life and the originating party should be made aware of when the data they generated will be deleted.
5.19	If IOT data is obtained from a third party, is the third party made aware when their data is resolved to another party?	When data is obtained from one party and resold to another, the chain of custody for the data should be provided to the originating party so inaccuracies and edits can follow the data trail.
5.20	If data is obtained from a third party and the third receives an incentive from the use of their data, is the transaction recorded?	When data moves between parties as a transaction, the movement of the data should be logged along with any

		incentives or other conditions that were attached to the transaction.

CONSENT AGREEMENTS

People are often willing to share data with the organizations that support their needs, however, they expect their privacy to be respected in such data exchanges. Since everyone has different perspectives on privacy, it is important to disclose to the individual the information they need to make an informed choice as to whether to share data or to withhold their permission.

6.1	Is a consent agreement sent/shown to an individual to obtain their consent to participate in a process that collects their data.	Data collection processes should only be used with the consent of those participating in the process.
6.2	When different forms of consent are collected on the same project, does the organization consolidate consent records to ensure consistent treatment of all subjects?	Different forms of consent are acceptable (e.g. phone, email, web site agreements) s long as the organization matches the right form of consent with the data to be collected, records are kept, and the consent processes include the key components of the consent structure
6.3	Does the consent agreement describe the data to be collected, describe purpose, and use of the collected data?	Consent agreements should make it clear to an individual why the consent agreement is necessary. Each consent agreement should be complete on to itself and be sufficient and clear for an average person to understand
6.4	Do the consent agreements describe the need for the data and the processing that will be conducted with the data?	The consent agreement should not provide a laundry list of possible uses but should be explicit and an accurate representation of the processes that will be carried out.
6.5	When the organization describes the use of the data in a consent agreement, is the description specific and reasonable?	Many data policies ask for a reasonable level of compliance but the definition of 'reasonable' is open to interpretation. The more specific the use description, the more likely the use description will stand up to shifting expectations of what is reasonable.
6.6	Does the consent agreement indicate where the data is physically stored and the identity of the organization responsible for maintaining the security of the stored data?	In today's world of outsourcing and cloud service providers, the chain of custody for data storage and processing systems is often complex. Individuals should be made aware if the organization makes use of such service organizations.
6.7	In large organizations, is the consent agreement clear which organizational divisions are associated with the consent agreement and who is the responsible party for the consent enforcement at that division?	The consent requests should always be clear about the organization desiring the consent and how the target may contact an individual at that organization if there are issues or questions.
6.8	Does the consent agreement indicate prohibited applications for the data or prohibited types of data sharing?	Consent agreements often focus on permitted uses of the data which can lead to ambiguity. While the consent agreement may describe permitted uses, if it fails to describe prohibited uses explicitly, this omission could be interpreted to imply that all other uses for the data are prohibited.
6.9	For some situations, the individual is given the choice to opt-in or opt-out of specific data collection processes. In these situations, opt-out should be the default and it should be clearly explained to the individual whether their decision to opt-in or opt-out will provide extra benefits or result in the loss of certain benefits?	Any opt-in/opt-out decision should default to opt-out if at all possible. Further the impact of the decision should be clearly explained so the individual understands how their decision will impact the level of service they receive from the organization (or if the decision is not service impacting)
6.10	The consent form should make it clear the user cannot impose any requirements on the organization based on their consent or their withdrawal of consent?	Just like organizations cannot hold services hostage to an individual in exchange for data unless the data is required, the individual should not be able to hold the organization hostage in exchange for special treatment
6.11	Is it clear that consent is only required for data that is necessary to complete a service and optional for additional data?	If the data is needed to perform a function that the user has requested, the organization should make it clear the completion of the individual's request is contingent on acquisition of the data. Data that is not absolutely necessary for that function should not be used as leverage for access to a desired capability
6.12	Does the consent agreement indicate whether the data will be used to engage in direct marketing to a user (sending commercial messages)? Can the user opt out of this use of their data?	The consent agreement should describe how collected data will be used. It is possible the user will approve of using their data for product research but might want to allow the organization to use the data to drive marketing programs. The individual should be given the opportunity to deny or allow specific uses of collected data.
6.13	Does the organization obtain consent before engaging in fundraising with a user?	Not all marketing is intended to facilitate sales of products or services. Before a non-profit undertakes a fundraising drive,

		they should ask for an individual's consent and then not engage the individual for fundraising purposes until after consent is granted.
6.14	Does the consent agreement identify any partners that might receive the data if the individual provides their consent?	Some people are willing to consent to a data collection process as long as the data stays within the organization but will not consent if the data is to be transmitted to a third party.
6.15	If a timely response to a consent request is not received, is there a defined process for following up with individuals in an effort to change an assumed no" to a definitive answer?	A non-responsive customer should be treated as though they formally declined to participate in a program that involves data collection, however, the organization may follow up with non-response individuals but it is important that the individual not be included in the process until a definitive response is explicitly received from the individual.
6.16	When the organization receives any form of consent from a user, is the identity of the user validated to make sure they are authorized to make such a decision?	Malicious uses can steal a person's identity, people share account access information, and some people seek to assert control over others. As a result, the person providing data may not be the person they claim to be. Organizations should attempt to assure themselves they are collecting with the person they expect.
6.17	It is important to validate that a requestor is permitted to submit (or withdraw) a consent request. Fraudulent requests or automated responses should be rejected. In the case of a situation where someone submits a request as a parent or a head-of-household, the requestor's authority to make the request should be validated.	Uses can steal a person's identity, people share account access information, and some people seek to assert control over others. As a result, the person providing data may not be the person they claim to be. When an organization receives a request to change the data they hold, efforts should be taken to ensure the organization is communicating with the person they expect.
6.18	Has each of the consent forms been explicitly signed and dated by the user? If electronic signatures are used, has the identity of the signing party been verified?	Consent agreements should be treated as legal documents and as such they need to be signed by the involved parties. If the document was 'signed' electronically, the log that lists the signing data should indicate how the organization validated the signing party.
6.19	If the organization uses electronic consent agreements, is it possible to reproduce the agreement in paper form at a later time in case it is called into question legally?	Electronic consent agreements are a viable form of record keeping but it is possible the individual may want to request a physical copy of the consent agreement and this should be possible. Further, it should also be possible to generate physical copies of a consent agreement when these documents are requested by a government agency.
6.20	Are users given copies of the signed consent authorization agreements) digitally signed or physically signed)?	Once a consent agreement is approved, a copy of the consent agreement should be delivered to the individual and saved by the organization as a matter of record. This document serves to document the date when the individual and the organization made the consent agreement official.
6.21	Consent agreements are normally triggered by initiation of a new data program. Once consent has been established, at a future point in time can the users ask for copies of the consent agreement?	When there is an open consent agreement between an individual and the organization, the organization should have a scheduled process to remind the individual about the open agreement. However, the individual may want to ask for a description of the agreement out of the scheduled cycle or even after the agreement has been closed.
6.22	Does the consent agreement describe how the user might rescind or alter their consent?	Individuals may change their mind about an active consent agreement for a number of reasons. It should be clear to the user how they can rescind or alter any established consent agreement.
6.23	Does the consent agreement forms list an explicit expiration date or list other specific events that would terminate the consent agreement?	When an individual provides their consent to participate in a program that allows data collection, that consent cannot be assumed to be valid indefinitely. Consent forms should not be open ended and should detail agreement termination conditions.
6.24	Does the consent form make it clear the data will be deleted once the mission outlined in the consent form actions are complete or does it give a date for when the information will be deleted (retention period)?	Individual information should not be treated as permanent data but as data with an expiration date. After a specific specified date or when the project is complete, the data should be considered stale and deleted. e consent agreement process should clearly explain the deletion event triggers
6.25	When user consent is needed, is there a consent form and does the consent form offer the end-user's a clear set of choices open to them with respect to the level of consent offered?	Consent forms should be specific (not broad and general) and they should be clear when describing the use of the data, the result if consent is not provided, and in the identification of the third parties that the data will be shared with.
6.26	At the time of consent, are data subjects informed of the procedures for changing their consent decision, reviewing any	Users change their mind after providing (or denying) consent. As a part of the consent process, users should be told how to

	collected information to date, and requesting a change of information? These instructions should be clear for the average user and usable?	change their consent decision and how to review and correct information that pertains to them.
6.27	When the organization is seeking consent to collect data from an individual, does the organization communicate the individual's rights under the organization's privacy/security policies and offer to answer questions relating to the data collection process?	As a part of the consent process, the organization should provide information about the individual's rights and offer to answer any questions the individual might have about the data collection process. These instructions should be understandable and easy to read and comprehend.
6.28	If the data collection process collects information from children younger than a specific age, does the organization have a policy in place that seeks to obtain parental/guardian consent before allowing the minors to provide data?	Guardians are expected to supervise children and others requiring oversight. This supervision responsibility extends to online activities. If the process collects data from someone who should be supervised, be sure to determine the responsible supervisory party and validate activities with that entity.
6.29	Children are not able to enter into a legal agreement such as a consent agreement. Different laws and regions set different age and information limits but it is generally always better to get consent from a guardian.	Guardians are expected to supervise children and others requiring oversight. Be sure to record approvals and disapprovals of any agreements as the children's approval in itself is insufficient.
6.30	If the data collection process collects information from individuals younger than a specified age, does the organization's policy afford these people special privacy provisions that might not apply to older individuals?	Data that is collected from protected cohorts should be flagged as data that requires a higher level of oversight. It is important that this data not be comingled with generalized data in a way where these special protections would be lost.
6.31	Young people are often early adopters and open to trying new things. This makes them vulnerable to predatory practices and organizations could benefit by making it clear that their data practices afford impressionable individuals special kinds of support.	Extreme care should be taken if any data from a protected cohort is ever given to a third party. Regardless of the care a data collection process provides in dealing with these cohorts, if a third party does not have sufficient protections, the data will not receive the protections it requires.
6.32	Some data collection programs that are targeted to adults may be accessible by children. If there is the potential for children to access the program, the organization should have a policy that attempts to validate that the participants are not children.	Data collection processes that are targeted at adult populations are often accessible by protected cohorts such as children. Data collection processes aimed at general populations should take steps to make sure their processes are not being accesses by unapproved individuals.
6.33	If the organization is attempting to collect data from children, does it have a process to make sure children are not lying about their age on a consent form?	Organizations should not simply ask the age before asking for consent. They should attempt to validate that the age given is accurate.
6.34	When consent is given, is it clear whether the limits of the consent apply to an individual, a group, a division, a company, or a group of companies?	Consent agreements should be specific as to who has access to the data. For example, is consent given to a specific person, a group of people performing a similar job, or the entire company? In a medical setting, is the consent for a doctor, a healthcare team, an affiliated set of practitioners, or an entire hospital?
6.35	If the data is to be sold to an outside organization or given to an outside organization that will sell the data, will the consent agreement allow the user to prohibit the organization from using their data in this way?	Users should have the ability to deny an organization the right to sell their data. This includes denying the organization the ability to give their data to a third party that would sell their data.
6.36	When collecting data, does the organization record the 1) home location of the data subject, 2) location where the data was collected, 3) the citizenship of the resident so that the organization can ensure the appropriate rules are applied to the data?	Different laws are applied differently depending on the residency, location, and nationality of the subject. If this information is not known, it is impossible to know which rules apply to the data
6.37	If the organization expects to be compensated for the sale or use of consumer data, is the consumer made aware of the value their data represents to the organization?	Many times people are unaware that their data is being sold or not made aware of the value of the data. This information should be disclosed so people can make an informed consent decision.

6.38	If the organization intends to sell or share information with a third party, does the agreement make it clear whether and how the user will be compensated for their data?	If the organization wishes to sell an individual's data or share it with a partner that will benefit from the data, they have the right to expect the benefits will accrue back to the individual. It is safest to state in the consent agreement how they will benefit from the data transaction.
6.39	Do the procedures ensure that the organization has asked and received consent from a user before it begins to collect their data?	Not all users will respond in a timely fashion when asked for their consent to participate in the data collection process. An organization can start to collect data as soon as an individual provides their consent but not until then. If consent was requested from multiple parties, the organization can wait until all responses are received or they can start the program and expand as responses come in.
6.40	Does the system record the time/date of each opt-in or opt-out offer and response?	Some systems are opt-in and some are opt-out. Opt-in systems explicitly ask participants if they are willing to share data whereas opt-out systems ask users if they wish to NOT participate. It is important to record, for each possible participant, when they were given an opt-in or opt-out opportunity.
6.41	If the organization makes use of electronic consent agreements, does the organization use a two-step consent process to validate the consent agreement?	When electronic communications is the only form of communications with a user, people may attempt to misrepresent themselves. After consent is agreed to, the organization should send a validation back to the individual to ensure that the correct person actually consented. It may also be important to assign each consent agreement a unique index number to validate the correct consent agreement was delivered, responded to, and validated against a validated document.

CONSENT FRAMEWORKS

A consent agreement is an agreement between the organization and an individual. The organization needs the individual's agreement to use their data AND they also need to have the capability to act on and otherwise support the individual.

7.1	Does the organization hold a formal review of its data collection needs before a new project is begun and does that review attempt to minimize the volume of personal data they maintain?	To minimize the impact of a potential data breach, the organization should seek to reduce the data it collects and maintains to a minimum. This means that each new project should be carefully reviewed to ensure that only absolutely necessary personal data is collected.
7.2	From the data policy, is it clear that services cannot be denied based on a consumer's willingness to provide data unless the data is needed to support the service need?	Information about user interactions with an organization's website may be stored in the form of cookies which are stored on the individual's computer or stored by the organization (or an affiliated partner) as a part of their data infrastructure. Since this information can be directly tied to a specific computer and the computer to an owner, this information should be considered as personal information.
7.3	If any of the data will be given or sold to an outside organization, to a partner, sold to a customer, or otherwise used by another organizational division, does the consent agreement describe what data will be given to each specific party and for what purpose?	If data is provided to different third parties for different purposes, each third party should be described in terms of the data they might receive and a description of permitted and restricted uses of the data by the third party so the individual involved with the consent agreement understands what will happen to the data they provide should it leave the organization.
7.4	If any of the data will be given or otherwise exposed to an outside organization, to a partner, sold to a customer, or otherwise used by another organizational division, does the consent agreement describe what data will be shared with each specific party and for what purpose?	If data is provided to different third parties for different purposes, each third party should be described in terms of the data they might receive and a description of permitted and restricted uses of the data by the third party so the individual involved with the consent agreement understands what will happen to the data should it leave the organization.
7.5	If the organization wishes to disclose the data to parties that were not listed in the original consent agreement, does it obtain a new consent agreement?	A consent agreement should indicate the third parties that might be given access to the data. If the list or permissible data partners should change during the process, the individuals should be notified of the change and given the opportunity to withdraw their consent if so desired.
7.6	Are Identities verified when an individual calls, mails, or electronically communicates with the organization?	When someone reaches out to communicate with an organization, the possibility exists that the individual may be masquerading as another person. The organization should have a mechanism by which it can validate the identity of an individual before accepting that a request from the individual is valid
7.7	When contacting individuals via mail, email, or phone, does the organization give the customers notices and consent information and is the conversation documented?	Consent can be achieved through the mail, phone, or electronically. No matter how individuals are contacted, there should be clear documentation that the customer was contacted, the information that was delivered, and the decision made by the individual
7.8	When contacting individuals via mail, email, or phone, about a privacy related issue such as breach notification or a change request, does the organization make it clear the notice is important and should not be disregarded as a marketing message.	In an age of over communications, many people disregard or scan incoming messages expecting many to be marketing or inconsequential messages. Messages related to privacy related issues should be clearly flagged as such.
7.9	If the system is based on opt-out logic, does the system explicitly confirm the opt-out decision with an independent message?	Users often overlook opt-out options and may believe they have opted out when they have not. It is always best to confirm an opt-out decision with a separate message to the participant.
7.10	If a consent change request impacts more than one party, is the request verified with the other parties before the change request is accepted?	Some collected data relates to a group of individuals such as a family or a small business. If data is being collected about such a group, care should be taken to ensure the party providing the data has been validated as being responsible for the group.
7.11	Users should be able to review and change erroneous data but the system should take steps to make sure the requested changes are legitimate and do not give rise to a data conflict. For example, if a married couple divorces and one party changes their marital status, data related to the other party might need to be changed as well.	If an organization receives a data change request that might impact group level data, the organization should take steps to either ensure the requesting party is authorized to act for the group or to seek validation from the other group members.

7.12	When an organization collects data from another party, there should be a documented chain of either consents or denials. Are the consents (and denials) appropriately documented? For a specific process can a consent/refusal of consent be generated showing the date the permission level established and who provided their consent?	A consent or denial record should show the date the response was received, the original request that was approved or refused, and an indication of the person who provided their consent (or denial). If the consent request had multiple options, the response for each request should be well documented.
7.13	Can people request a report from the organization about the data the organization maintains so they may review the data.	Many people are willing to allow an organization to maintain data about themselves but would like to have a mechanism by which they can review the data
7.14	When an individual's data is to be integrated with data from a third party, is the individual made aware of the integration process and the external data that will be linked to their data?	The consent agreement should describe how the information they provide will be used. This includes a description of how their data will or might be integrated with third party data.
7.15	When an individual's data is integrated with third party data, does the individual still have the right to withdraw consent, request changes, or deletion of the resulting integrated record?	When third party data is integrated with an individual's data, the individual's privacy rights cover the entire information record including the parts of the record obtained from any third parties
7.16	When the data policy changes, does the organization communicate the changes in the policy and give the individual the option to change their consent settings based on the new policy?	Data policies do change and the organization cannot assume that all individuals that have provided consent under the old policy will want to consent under the new policy. A new consent agreement must be obtained when the data policies change.
7.17	If the organization wishes to use the data for a purpose other than stated in the original consent agreement, does it obtain a new consent agreement?	A consent agreement should describe the data to be collected and how the data will be used by an organization. If these conditions change to new conditions or new types of data/processing will be put into practice, the individual should be given the opportunity to consent or deny access to data based on these new conditions.
7.18	Does the organization have a process by which a user can send a request to have all data about them edited or removed from the system (right to be forgotten)?	Users should be able to request a report about all data that an organization holds about themselves. If the user disputes the accuracy of certain data elements, they should have a process to contest and correct any erroneous data. They should also have the ability to request all or some of the data being held be deleted.
7.19	When a user requests to be forgotten, the request should give the user the option to request their data be deleted from one specific data set or from all data sets.	Data is often compartmentalized and held in different places and used for different purposes. A request to review data about a person should cover all data sets held by the organization. Requests to edit or delete data should be applicable across some of all held data.
7.20	When the organization receives a request to review data, edit/change data, or delete data related to them, once the action is complete, is a completion notification sent back to the user for revalidation?	It is possible that an organization receives a request to review the data held about an individual from a source which is improperly masquerading as another user. Organizations should always attempt to validate the identity of any user requesting a change to their data.
7.21	Requests that would require that the organization change the data about an individual or their consent agreements should result in the generation of a completion notification so the individual knows the request was completed and to give them the opportunity to raise an objection if they did not originate the request.	After a change request has been received and validated, the organization should make the requested changes across the appropriate data sets. Once the changes have been completed, a completion indication should be sent to the user to notify the user that the change has been carried out as expected.
7.22	Is data collected from third parties about an individual classified as being individual data so that requests for deletion or editing apply to third party and directly connected data?	Individuals have the right to request a review of all data pertaining to the individual regardless of the source of the information.
7.23	Does the organization's policies allow data subjects to withdraw consent to use their associated personal data at any time?	Organizations should allow individuals to withdraw established consent agreements or change the conditions of an established consent agreement at any time. The process for making such a request should be clear and easy to find on the organization's web site.
7.24	If the user wishes to withdraw consent, should the organization inform the user of any consequences of the withdrawal?	If the organization is providing a service to the individual and the individual withdraws their consent, the organization should

		describe how the change might impact the level of service the individual receives
7.25	Does the policy permit people to request a list of disclosures the organization has made about the person (and who got the information)?	Individuals should be able to request and receive a list of third party organizations that have received data about the individual.
7.26	Does the privacy policy make it clear that data will be disclosed to authorities when the law or court orders require disclosure and that laws and court orders can nullify specific organizational data policies?	If a valid court order exists, any collected data must be disclosed regardless of whether there is consent and the individuals should be informed that their consent or lack of consent cannot shield them from a duly authorized court order.
7.27	If a user withdraws their data-use consent, before any actions are taken, does the organization check to make sure the permission withdrawal will not result in a legal violation?	If there is a court order that requires an organization to report data exchanges to an officer of the court and withdraws their consent agreement, the court order may supersede the individual's request.
7.28	If consent is withdrawn, the consent withdrawal process should make it clear that the user has the option to request the data to be 1) destroyed, 2) locked and not used, or 3) blocked from further distribution?	Once the organization has begun collecting data about an individual under a valid consent agreement, if the individual withdraws their consent, the organization has to decide how to treat the data collected to date. The individual should be given the choices and allowed to select the action to be taken.
7.29	When the organization receives a request to review data, edit data, or delete data, is the request forward to all third parties that may have had access to the data and are those third parties required to confirm deletion/change of the records?	When an organization transfers data to a third party, if a change request is received after the transfer has been completed, it implies the data held by the third party is in error and the organization should correct the data held by the third party to ensure the remote data is an accurate representation of the individual(s) that have requested changes.
7.30	If a user requests a change to the data an organization holds and the change request is rejected, is the rejection reason documented? Are users able to comment on the refused change request and able to challenge the rejection?	There are legitimate reasons why a change request might be rejected. For example, if the organization no longer holds the data or if the change request refers to a data record that was modified after the change was requested. Another possibility would be if a family member requests a change to the family's consent status and that member is not authorized to make such a request. Regardless, it is important for the organization to acknowledge all requests and to cite why a particular request may have been rejected.
7.31	If the data processing or storage function is moved to another location is the user given an opportunity to change their consent agreement?	The consent agreement should indicate geographically where the data will be stored and where it will be processed. If the organization changes the storage location of the data or the processing location, the individuals with open consent agreements should be notified as an impacted party and then given the opportunity to withdraw their consent.
7.32	If data about a specific individual is to be transferred across a geopolitical border, the users often expect they have the right to object and to prevent such transfers?	Some people who might opt-in to a program might expect that their data will remain local where local laws apply. If an organization transfers the data to another county, the other country's laws may begin to apply and the user might wish to deny or withdraw their consent because of that.
7.33	Does the organization send privacy policy reminders to individuals on an annual basis to remind them of their rights associated with the active consent agreement?	People often forget about privacy policies and need to be periodically reminded. They also will forget what data is being collected from them and how this data is being used.
7.44	If a user detects that their data may have been used without their permission, is there a defined process by which they can complain about the issue?	When an individual provides consent, the consent agreement will specify how the data can be used and whether or not the data can be shared with third parties. If the individual suspects the terms of the consent agreement have been violated, there should be a process by which the individual can request the initiation of an investigation. At the end of the investigation, the findings should be sent to the requesting individual along with a description of any action taken before the request is closed.
7.45	If the organization is notified that an unapproved change was made to permissions or data, is there a log so the organization can investigate the source of the request in order to take corrective action?	If the organization is alerted that an unapproved change request was received, this could be an indicator that the data has been hacked. It is important that the organization be able to investigate such notices in order to determine if the change was a human error or an indicator of a more significant issue.
7.46	When users ask questions or complaints about a potential abuse of the data policy or a consent agreement, are those issues	The data policies and the consent agreement between an individual and an organization is important. When an individual raises an issue via the website, email, phone, or mail, the issue should be logged and tracked so the organization can later

	logged and tracked to make sure the user receives a timely response?	demonstrate that the issue was noted, investigated, and appropriate actions were taken. The expectation is that when issues are raised, they will receive a response within 30 days.
7.48	Does the organization have a policy that prohibits the organization from marketing/advertising inappropriate products or services to minors?	Organizations should be carefully to make sure that inappropriate advertising is not sent to minors by mistake
7.49	Does the organization specifically define the ages of what its policy considers to be children so that children can be afforded special privacy rights?	Different laws define children differently. Some laws consider children to be anyone younger than 15, others 16, others 18, and still others 21. The organization's privacy policy should define children to be a specific age.
7.50	Are there procedures that allow a guardian to give and withdraw consent for data collection from a person they oversee?	All children have legal guardians, however, occasionally adults have legal guardians as well. There are situations (e.g. elderly) where a legal guardian has oversight for an individual's legal rights. There should be a process by which a legal guardian can intercede on behalf of an individual they legitimately oversee. The process should be sufficiently secure to prevent a person from masquerading as the guardian of another as well.
7.51	Are there procedures that allow a guardian to give and withdraw consent for data an organization has about their children that can be released to an external organization?	All children have legal guardians, however, occasionally adults have legal guardians as well. Organizations should not release data about these vulnerable individuals without the consent from their legal guardian
7.52	Are there procedures that would allow a parent/guardian to delete or edit records about their wards?	Parents should be able to change data about their children or others they oversee.
7.53	Does the policy determine when and if ads can be delivered to children? Does the policy determine when and if ads can be delivered to parents/guardians of the children?	Targeting ads to children is problematic and should not be done especially if the ad is encouraging a behavior that the parents/guardians may not condone. Some ads/messages are better sent to the parents/guardians.
7.54	When IoT devices that will connect to the network are shipped to someone, the packaging should provide a brief description of the data to be collected and how it will be used.	It cannot be assumed that people will go online to read the privacy policy. When someone get a device that will connect to the internet and generate data, the packaging should provide an overview of the data protection policy.
7.55	Does the organization feed any collected information back to the respondent to give them a chance to verify the data before it is stored?	When users provide data, there can be typos and other types of data errors that could introduce errors in the data. Respondents should be given a chance to correct any such collected data at the point of collection.
7.56	Does the organization use Social Security Numbers to identify specific individuals?	Individuals should never be referenced by their social security number (SSNs) and SSNs should never be displayed or listed in reports of any kind. If SSNs are needed for taxing purposes, they should always be encrypted or masked.
7.57	Does the organization use driver's license or other DMV identification information to identify specific individuals?	Driver's licenses can be used to verify other information but the driver's license numbers or other DMV identifiers should not be stored or used to identify individuals for anything other than DMV or other legal purposes.
7.58	Does the organization use identifying information from one consent agreement to solicit consent agreements for another purpose?	Individual identification information collected under one consent agreement should not be used to collect consent agreements for another purpose. Consent agreement data can be used to notify users of matters related to the existing consent agreement but not go beyond the uses described in the original agreement. However, a consent agreement may include an optional clause asking for consent to contact an individual for other purposes that may require additional consent.
7.59	Is there a process by which a user can export the data an organization has about them so that they can give their data to a different service provider?	There should be an easy means to transfer data about one person from one service provider to another.

EMPLOYEE/STAFF ISSUES

It should be clear in the employee handbook that employee data privacy is not an absolute right. Monitoring employee productivity may be needed to generate the data that serves as a basis for pay or promotion programs. Despite the fact that employee data privacy is not a personal right, the employee should be aware of what behaviors and conditions are being monitored. In addition, there are some situations when employees should expect privacy (e.g. when using the restroom) and some situations where they should expect heightened privacy protections (e.g. healthcare related activities).

8.1	Does the organization structure employee access permissions based on rings, organizational silos, levels, or per user?	Security rings or layers classify data and users based on their permission in a ring structure where those within the innermost ring have the greatest permission levels. Hierarchy structure defines clusters in alignment with the organizational hierarchy. Ad hoc assigns permissions for each user separately.
8.2	Does the organization provide a whistleblower hotline system where people can report situations that might pose a privacy/security risk?	Many breaches are often the result of a process that is not being properly followed and by human error associated with carrying out these defined processes. People should have a mechanism to report possible wrong doings so steps can be taken to address potential issues before they can develop further
8.3	Does the organization provide a help desk for customer/employee use?	Privacy and Security are complicated issues with many nuances. It is possible that someone will carry out an intended process incorrectly because the process was not completely understood. There should be a mechanism by which people can ask for help to better understand a process in order to avoid making a misstep.
8.4	Is there a process by which employees can see the data the organization holds about them and given the opportunity to make corrections?	Employees should be able to see the data the organization holds about them, given the opportunity to make corrections, and receive data breach notifications.
8.5	When employees are terminated from the organization, are there data rights immediately terminated?	Whenever an employee leave an organization or if an organization's partner is disassociated with the organization, their access to the data systems should be immediately terminated.
8.6	Does the security process insist on a two factor authentication for employees?	Employees often have to access data records remotely. This means that extra care is needed when organizations support remote access to data. Two factor authentication includes a range of techniques that can be used to verify someone's identity before access is granted to the system.
8.7	Is it clear to employees that any efforts to deceive the organization with respect to data use or permission justification is considered a serious issue and may result in disciplinary measures?	Organizations should consider employee privacy/security transgressions are a serious issue and represent grounds for disciplinary measure including termination.
8.8	Does the organization make it clear that the private information used to recruit and manage personnel is covered by the organization's privacy/security policy even though the individual is not currently an employee of the organization?	The application and employment processes should make it clear to the prospective/current employees that the organization will be collecting and maintaining certain necessary data and consent is implied as a condition of application for employment.
8.9	Does the organization treat private-sensitive data about employees and customers with the same level of regard?	There is much in the press about disclosure of customer data, data related to the employees of an organization is just as sensitive. In an employment setting, data is a normal part of hiring, managing, and termination employees. An organization must collect and manage a lot of data about employees to manage their employees and this data needs to be managed securely. The policies associated with managing employees should be disclosed to the employees including volunteers, contractors, interns, etc.
8.10	Does the organization seek employee consent before collecting data that is not required for employment?	Organizations can collect employee data without the consent of the employee as long as it is necessary to establish, maintain, or terminate an employee-employee relationship. Other employee data which might be collected by the employer requires consent.
8.11	If the organization outsources certain employee management functions, does the organization secure commitments from the outsource company to honor their data	Outsourcing employee management functions does not free the organization from its responsibility to ensure employee data privacy. If the company outsources service functions, a part of

	policies before they provide access to employee data?	the outsource agreement should include a requirement that the partner support the organization's privacy/security policies.
8.12	Does the privacy policy put specific limits on the use of employee location tracking?	If an organization uses tracking technologies to aid in employee communications or to monitor productivity, the tracking information policies should include times/situation when it is used and specify sunset provisions that require an organization to delete historic data after the sunset period has expired
8.13	Does the organization's employee privacy policy describe how the organization might use of audio and video technologies to monitor employees?	Organizations can monitor employee actions but they should make the employees aware of the surveillance practices and they must limit the use of such technologies in situations where employees would expect privacy (e.g. restrooms, changing rooms, etc.).
8.14	Does the organization's employee privacy policy describe how the organization might monitor employee computer use and on-line activity (including email and social network monitoring)?	Organizations can monitor employee online/computer actions (e.g. tracking websites visited, files accessed, social network use, application use, etc.) but they should make the employees aware of the surveillance practices.
8.15	Has the organization defined situations when monitoring employee activities would not be permitted?	The organization's policies should explicitly limit the use of such technologies in situations where employees would expect privacy (e.g. restrooms, changing rooms, etc.).
8.16	Does the organization post signs in areas where video surveillance technology is used so customers and employees are aware they are being monitored?	Clear signage should be used to notify people of any active monitoring programs should also be posted in monitored areas so they can avoid those areas if they have a privacy concern.
8.17	Does the data policy prohibit employees from taking sensitive data off premises?	Risks associated with a breach of data privacy/security is significantly increased when data is taken out of the organization's physical purview. To reduce these risks, the organization should consider taking actions to prevent data from being taken to remote locations or accessed by remote data processing systems.
8.18	Does the organization have documented policies and procedures detailing who has access to employee data and how employee data can and cannot be used?	Employees with access to data related to staff are different from employees with access to customer, partner, or product use data. Employees with access to employee data need to be tracked and managed independently from employees with access to data related to the organization's products and services.
8.19	Does the organization minimize the risk of exposure by limiting access to sensitive data to those with a documented need to know?	Access to personal data should be controlled and managed on the basis of a need to know and least privilege. The access management process for personal data should be integrated into the enterprise's overall identity and access management processes. Roles, functions and individuals with access to personal data are identified and managed accordingly.
8.20	If the organization does credit checks on employees or prospective employees, does it obtain their consent before running the checks?	Employees do not need to consent to a credit check when the check is for employment screening purposes, however, it is a good idea to seek the employees consent and they should delete this information at the earliest possible moment.
8.21	Does the organization "test" Phish with the employees in an effort to identify employees who might need additional training?	Some security breaches are the result of an employee accessing an email or a web site with an embedded Trojan horse. Simulated Trojan horse emails can be used to train employees on Trojan horse detection, improve employee's readiness, and to provide defense readiness metrics.
8.22	Are the employees kept up to date on the most recent email, website, and phone phishing threats?	The world of cyber security evolves quickly. Employees and often customers are the first line of defense for any organization. To keep these individuals alert and cognizant of the latest threats, periodic updates should be a part of the policy.
8.23	If the organization makes use of spam or other filtering technologies, is it clear to the users how this technology is being used and which messages might be filtered?	Blocking of messages thought to be spam may be well intentioned but opens the door to what might be legitimate private communications. Consent and proper disclosure may be needed before these technologies can be activated.
8.24	Does the organization's data policy prevent them from releasing employment data to a third party without employee permission?	Employee data is personal data and data should not be released to a third party without the consent of the employee. If the organization does have a policy of releasing limited employment data such as start and termination dates, the nature of the data that might be released without employee consent should be well documented.
8.25	Does the organization use technology to track/monitor employee location?	Location monitoring technology can be used to facilitate clock-in functions or to find key personnel during an emergency. This is an acceptable use but the employees should be made

		aware of the technology and any limits placed on the use of the technology.

BREACH ISSUES

Data breaches happen. No matter how much time and money an organization puts into data privacy and security, there is the possibility a breach will happen. The data governance policy should accept this and be organized with a rapid response plan that can be quickly activated in the face of a data breach.

9.1	Does the data breach notification processes begin if there is a reasonable belief that unencrypted or encrypted data with the decryption key was obtained by an unauthorized person?	A breach implies improper access to unencrypted data or improper access to unencrypted data and the decryption key needed to make it readable is a possibility. Even if there is not absolute evidence of a breach, the notification process should be initiated once there is a reasonable possibility a breach occurred. Note that if law enforcement officials ask that the notification be delayed so that they might investigate, the notification process should be delayed but the reason for the delay should be included in the notification once the process resumes.
9.2	When a data event occurs, an incident file should be opened to document the event and the actions that arose as a result of the event. Does the occurrence of an event result in the creation of an incident file?	The chief privacy/security officer's office should have a set of incident files. Some may be open and active and others may be marked as closed and complete.
9.3	Are data breaches classified by their potential impact so the reaction protocol can be based on the potential for the breach to do harm?	The reaction to a detected data breach should be dependent on the breach's impact to cause havoc and the data policies should reflect this. For example, the policy might indicate that if a breach impacts more than 500 individuals a data breach report should be sent to the attorney general. Alternatively, if the data breach subjected the organization to digital blackmail, the response might call for a response that includes the police (a crime has been committed) and the organization's finance personnel (since money is involved).
9.4	Does the organization have documented and implemented breach response plans in place?	Data breaches often represent a time of crisis. When faced with such a crisis, the response will need to be both appropriate and swift. The response team should not have to develop a response plan in response to a situation, they should have a documented response plan in hand that they can efficiently execute against (and modify if needed)
9.5	Does the data breach notification process set specific time thresholds that trigger when a) management is made aware, b) when government authorities are made aware, and c) when the individual is made aware of a potential data breach?	While specific thresholds for data breach notifications will vary based on severity and the potential negative repercussions of a data breach, the guidelines for such notifications should be clearly identified in the organization's data breach reaction procedure.
9.6	During a data breach, a response team is formed that will consider a specific data breach and report to management.	The outputs from these security/privacy breaches meetings should be documented. Does the documentation indicate that the team worked to identify the cause, created a recovery action plan, created a preventive action plan to make sure the breach is not become an recurring activity, and does the document show that the recommended recovery actions have been pursued to completion
9.7	Is there a process by which a list of individuals potentially impacted by a data breach can be quickly put together?	During a data breach, time is important. If it is difficult to create a list of potentially impacted individuals, the organization's ability to issue a timely data breach notification may be impacted.
9.8	Does the data breach notification policy specify that historic customers and partners should be notified of a breach that might affect them even though the organization no longer has an active relationship with them?	Organizations often hold data that describes historic interactions with individuals and partners the organization no longer has a relationship with. Should a data breach have the potential to impact these legacy individuals, data breach notification policies should be followed as a matter of course.
9.90	Does the organization have a data breach reaction plan that includes an escalation plan that tells employees which level in management needs to be made aware of the detected incident?	The organization should have a documented data breach reaction plan that prescribes a response plan that should be followed when a data breach is detected internally or reported to the organization from an external source. The plan should seek to immediately stop the data breach and then attempt an initial determination for the possible extent of the damage. This information should be conveyed to the appropriate manager, based on potential impact, so a response team can be marshalled.

9.10	Is there a data breach notification template that can be quickly adapted for a specific situation to ensure a smooth and rapid response to any such breaches?	During a data breach, time is important. If the data breach response team has to take time to craft a data breach notification letter and then obtain management approval for the letter during the crisis, precious time may be lost. A data breach notification template that can be pre-approved before any detected data breach can serve to improve data breach response times.
9.11	Have all the proper governmental authorities and their contact information been pre-defined on a contact list to allow for a rapid response?	During a data breach, pressure is high and a timely response is important. Key contact points should be documented along with any breach reporting requirements so the response team can react quickly and with professionalism
9.12	Does data breach notification policy describe when and what information must be provided to government authorities and by extension, which data should be withheld?	Organizations often must disclose information about a data breach to the government; disclosure of this data does not require customer consent but it should also not disclose more information than is required. The organizations should disclose what is required but not volunteer extra information that might violate individual consent agreements or data governance policies.
9.13	When information about a breach is provided to the government, are steps taken to make sure affected individuals are aware that the government is aware of the situation?	Some data breaches require that notification be sent to government agencies. Individuals that might be potentially impacted by the data breach have other notification requirements. The fact that a government agency has been made aware of a possible data breach could mean the government has data about these individuals and therefore the individuals should be made aware of the government's involvement. There should be clear rules about when individuals are made aware of government involvement that might stem from a possible data breach
9.14	If the data breach response process involves law enforcement officials, does the data breach notification process give law the opportunity to intercede in the process?	If law enforcement officials ask that the data breach notification process be delayed so that they might investigate, the notification process should be delayed but the reason for the delay should be included in the notification once the process resumes.
9.15	Does the data breach notification process clearly indicate when a breach report should be sent to the impacted data subjects?	The organization's processes should define whether the notice is sent to individuals that have the potential to be impacted by a data breach. The process should specify whether the individuals are contacted via email, letter, notices on a website, text, phone call, or some other method.
9.16	Does the data breach notification policy describe when and what information must be provided to customers/end-users?	Depending on the situation, a data breach may require the organization to notify potentially affected individuals. In general, these individual notifications should include a normalized descriptions of what happened, what information was potentially disclosed, what the organization is doing in response, any action the individual should take, and provide a contact point if the individual has questions or needs more information
9.17	Do the breach notification messages provide management, government authorities, and data subjects appropriate contact information for use if they have questions or concerns?	When a data breach notification process is initiated, it can be expected that the notice will create concern. It should be clear to people receiving a breach report how they can reach out to the organization in order to get a timely response to questions they might have.
9.20	Has the organization provided sufficient budget for the data governance team to ensure money is available to analyze unexpected data breaches and take corrective actions in the face of an unanticipated data breach?	If the organization's budgeting process fully allocates the available budget to defined capital and expense projects, there will be insufficient budget available to allow the organization to respond to an unforeseen data breach.
9.21	Is the data protection office funded to conduct data breach testing and assessment exercises?	Data protection/privacy governance is an exercise in readiness because one does not know when or what form the next data breach will take. This means that organizations should conduct readiness drills. The data protection office should be funded to carry on periodic readiness training exercises.
9.22	Does the organization have cyber liability insurance to cover the costs associated with recovering from a data breach?	It is hard to predict the cost of a data breach. When faced with a data breach, the situation must first be stabilized, corrective action is needed to repair any damage, and take preventative action to reduce the potential for recurrence. If an organization does not have access to the funding needed to support these activities, they should consider obtaining insurance so a data breach does not damage the fiscal integrity of the organization.

9.23	Does the organization have insurance that would include funds to implement a make-right consumer program after a data breach?	It is impossible to guarantee that data security will never be breached no matter how vigilant an organization might be. Given that such a possibility is always present, an organization should consider obtaining insurance so the costs of responding to such an event do not impair the organization's finances.
9.24	Does the organization keep records of all security and data breaches?	Security and breach records are important. This information should be sufficient to allow forensic analysis and trends analysis. In addition, this information may be needed if an internal or legal investigation is to be conducted.

AUDITING PROCESSES

Having a good privacy and security program is meaningless if you cannot assess how well it is working. It is important to audit the intended and aspirational goals in order to determine which processes need improvement. Ideally each year the program will be improved in the spirit of continuous improvement

10.1	Does the organization review active projects to determine whether processing is actively being performed in accordance with the originally documented data processing privacy requirements?	Programs that utilize personal data should be checked for compliance with the organization's data governance program at its inception and then periodically reviewed while the program is active to ensure the originally designed processes are being adequately followed.
10.2	Is there evidence that the chief privacy/security officer's office conducts periodic audits of the different aspects of the data governance framework to ensure adherence is being maintained? Are periodic reports transmitted to management to alert them of potential issues and to report on progress to improve overall readiness?	Threats to privacy/security will happen - it is unavoidable. To maintain a state of readiness, the chief privacy/security officer should conduct data privacy and security drills, evaluate processes for adherence and sufficiency, in order to be on a path of continuous improvement.
10.3	Does the organization's data policy require the organization produce periodic (e.g. annual) security/privacy reports? Is it clear how these reports are made available to the appropriate parties?	Management needs periodic reports about data governance issues. Some organizations may want to make summary information available publically or in their annual reports. In addition, some regulations have specific requirements about the need for regular security/privacy reports.
10.4	Does the organization's regularly scheduled privacy/security audit also include an assessment review that serves to identify areas for improvement, create an action plan, and then follow up to ensure the actions are completed?	Regularly scheduled audits are important to make sure existing policies are being followed. These audits should also serve as an opportunity to reconsider existing policies in an effort to identify areas for improvement so the organization's policies are continually being improved.
10.5	Going beyond regularly scheduled audits, does the organization's policies should automatically trigger an out-of-cycle data protection impact assessment review whenever new technologies and systems are introduced or upgraded in the data processing infrastructure?	Whenever new technology is introduced to the infrastructure and complete assessment should be triggered to make sure a) the new technology is acceptable and properly configured to reflect the organization's needs, and b) to make sure the new technology does create a need to change other infrastructure systems or policies. Notes of such meetings should be documented and made a part of the record
10.6	Does the organization's policies allow management to initiate an out-of-cycle data protection impact assessment review when they have concerns that may have been raised by an anonymous employee, customer, or partner?	Any member of the management may receive a report of a potential issue that is of concern. Management should be able to trigger an investigation without being forced to reveal the source of the matter that raised their concern.
10.7	Does the organization's policies allow employees involved in data processing to initiate an out-of-cycle data protection impact assessment review?	The employees involved in data processing systems often understand the risks associated with the data they are dealing with. It should be possible for these employees to trigger an audit to ensure the data is being adequately protected if there is concern that the data they work with might create a future cause for concern.
10.8	A data governance committee should meet periodically to review data governance audits, action taken on any detected data breaches, to consider preventative actions, and other issues necessary to protect the data which the organization is responsible for. Are outputs from these meetings documented?	Periodic meetings of the management team involved or impacted in data governance is important. There should be evidence that important issues have been identified, that action plans have been created, and that open action plans are being monitored.
10.9	When examining a specific data set, is it clear which individual and group(s) have access to that data and how an approved user may be contacted?	When a data breach is detected, often the impacted data sets are often the starting clue. The organization's staff should be able to trace back from a data set to find users with permission to access that data so they can be alerted to the breach.

INFRASTRUCTURE SECURITY ISSUES

Data Management Governance includes two related but distinct fields: Data Security and Data Privacy. Data Security strives to ensure that bad people do not obtain data that they should not have and data privacy strives to ensure that data is only used for purposes that were understood and approved by the original owner of the data. Within that, infrastructure security manages the underlying networked resources while systems security manages users and usage of the systems

11.1	Does the organization believe it provides what it considers to be a "reasonable" measure of data security?	Some organizations understand their operational processes are problematic but suffer to find resources (time, money, expertise) needed to put identified action plans into effect.
11.2	Are critical computing devices identified as such and are they physically secured so they cannot be stolen or tampered with?	Critical devices should be locked so they cannot be accessed or physically secured with all access ports disabled.
11.3	Does the organization require that users register new mobile devices before they are permitted to access the network?	Mobile systems, by definition, are hard to track because they are not always connected to the network and they are not in a fixed location. Mobile devices should be registered ahead of time so the system knows when an identified system is being reconnected to the network or when an unknown (and unsafe) device is first identified.
11.4	Are mobile devices with access to sensitive data precluded from storing the data on the local device?	As wireless technology becomes more capable, remote/portable electronics become more capable. If these devices are able to store data locally, they become potential points of risk if the devices are lost or stolen. Privacy/security constraints on portable devices should be more stringent than devices that can be secured in a specific physical location.
11.5	Should the organization's systems resist efforts to copy sensitive data to portable storage devices (portable drives, jump drives, local disks, etc.)?	Local storage devices should as jump drives, portable drives, and other devices are designed to make it easy to move data from one machine to another. These same devices also make it easy to lose track of sensitive data that should be carefully protected.
11.6	When the organization removes a device from service, are the memory and drives securely wiped or physically destroyed? Is there are process for equipment removal?	There should be a defined device removal process so that retired devices cannot be disassembled so their piece parts can be scanned for passwords or other sensitive data.
11.7	Does the system detect and alert operators when unexpected activity is detected such as a) higher than expected traffic patterns, multiple log-in attempts, abrupt log-out activity, etc.?	All systems have expected patterns of behavior. When unexpected levels of activity of any kind are detected, these could be early indicators of worrisome behavior that might signal an effort to get past privacy or security controls
11.8	When a device, file, or jump drive is lost that may have sensitive data, is there a process for staff to report the loss?	It should be quick and easy for employees to report the loss or the suspected loss of data that might be on a stolen computer, disk drive, jump drive, etc.
11.9	Can lost or stolen devices be geolocated (lojack-like) so that they can be remotely erased?	Many devices have location tracking capabilities. If these systems are made visible to the organization's data security staff, lost or stolen devices can be tracked. Further, if the security staff is given appropriate access, lost or stolen devices can be remotely wiped to impair efforts to steal the data contained within the device.
11.10	The organization should have the means in place so that any device that is suspected of being infected can be quickly isolated and blocked from further access to the network?	When a data breach is detected, the first action should be to contain the data breach so that it cannot be further spread within the organization.
11.11	Is there a record to show that all the devices have been checked to make sure their firmware is up to date? Is there a record for each device that shows the last firmware update and date it was installed?	All devices with network connectivity should be periodically checked to make sure their firmware is up to date and has not been modified by some outside process or person.
11.12	Is there documented evidence that all computers and other devices have been regularly scanned for malware?	Devices should be checked periodically for viruses and malware. Further, records should be maintained to simplify the process of identifying at-risk machines after a security breach has been detected.
11.13	Are firewalls in place, active, and periodically updated across all network access points?	Firewalls should be installed at all network access points, the software should be kept up to date, and their configurations should be examined to make sure they are a reflection of the organization's current recommendations.

11.14	Is access to the backup systems tightly managed so that only specially authorized employees have physical and logical access to the backup systems?	Backup systems are often the last line of defense and this makes it important to ensure the backup systems cannot be intentionally or unintentionally corrupted. This is best done by providing minimal access to these systems to only the most trusted employees
11.15	Are the data backup systems tested periodically?	Backup systems become important if there is a data breach and the organization wants to recover based on historic (pre-breach) versions of the data. To make sure these systems work, they should be periodically tested.
11.16	Are back-up data systems physically secured and physically inaccessible by unauthorized users?	If during a data breach the backup data sets are impaired, the backup system can be obsoleted. To ensure that hackers cannot completely destroy the backup files, a higher level of access control is needed for the archival system.
11.17	Does the organization have an Internet-of-Things (IoT) deployment policy?	IoT devices create a significant amount of data that organizations are often dependent upon. Many IOT devices are remote making them susceptible to hacking or infection from malware. When a new IOT device is deployed, its physical location along with any hardware and software descriptions should be documented so that an auditing process can periodically evaluate each device for software/network safety.
11.18	Are any data transmission lines and network systems that might carry sensitive data encrypted?	When data is transmitted it can be observed and copied unless the data is encrypted before the transmission.
11.19	All wireless access systems (Wi-Fi, cellular, Bluetooth, other), even guest access, encrypted?	Nobody should be able to access the organization's wireless network without explicit permission from the hosting organization.
11.20	If unsecured guest access to Wi-Fi or some other wireless technology is allowed, that network should be completely isolated from the organization's internal-use network?	There are times when an organization might want to support an unencrypted network. In such situations, it is important that the unsecured network is completely isolated from the organization's internal operational network.
11.21	Is each IOT device password protected and has the password for each device (computer, mobile, IoT) been changed from its default so that each device has a different password?	Most modern devices that can be connected to an organization's network infrastructure can be remotely managed. Access to these device management features are password protected. When a new device is obtained, the password on these devices should be changed from the default before it is connected to the network. Device passwords should be stored in an ultra-secure location.
11.22	Are the IT centers monitored by video?	Video surveillance should be used in order to identify individuals who may have taken an inappropriate action.
11.23	Does the organization monitor network traffic volume and compare it against expected norms?	When observed traffic volumes exceed expected norms, this could be an indication of a cyber-attacks and the overage should be investigated.
11.24	Is the network scanned periodically for unidentified devices?	Devices that have not been properly scanned for security issues may be periodically found on the network. The network should be scanned for unknown devices and their access should be blocked until they can be identified, scanned for security flaws, and added to the inventory.
11.25	Does the organization track and report statistics related to cybersecurity threats?	Statistics are important as they allow trend analysis and can help steer future cybersecurity planning efforts
11.26	Does the main IT center have an emergency backup power system which allows IT systems to run despite a possible power outage	Power surges and outages are a fact of life and data is the lifeblood of many organizations. Interruptions to commercial power should not be able to disrupt IT operations.
11.27	When system components have been taken off-line for testing or maintenance, are they re-tested for security integrity before being reconnected to the operational network infrastructure	The system should normally be monitoring itself for possible security threats but when a part of the system is disconnected from the core it is no longer being actively monitored. Therefore it should be rescanned before the equipment is reintroduced to the system
11.28	Does the organization only work with cloud or other virtual system providers that provide an adequate level of security?	Cloud and other virtual systems are based on reuse of resources. Virtual machines are constructed from virtual resources on an as needed basis. Processes should be in place to make sure such virtual resources meet the security standard applied to physical resources.
11.29	Has the organization's internal network been sectored so a breach of one portion of the network is insulated from the rest of the network?	Networks can be segmented by geography, floor, department, or function. If these segments are managed as independent sectors that link through a protective layer, damage from a breach can be isolated.
11.30	If Blockchain technology is used to manage a distributed data structure, has each blockchain node operator been audited for	Blockchain technology supports secure communications between distributed nodes that are tied together via a secured communications system. However, it does little to ensure the

	proper privacy and security policy adherence?	operators of these distributed nodes are secure or maintain proper privacy practices. Unless the node operators are being audited for proper practices, the data structure can be corrupted and integrity can be disrupted.

SYSTEMS SECURITY ISSUES

Data Management Governance includes two related but distinct fields: Data Security and Data Privacy. Data Security strives to ensure that bad people do not obtain data that they should not have and data privacy strives to ensure that data is only used for purposes that were understood and approved by the original owner of the data. Within that, infrastructure security manages the underlying networked resources while systems security manages users and usage of the systems

12.1	If the organization assigns data access privileges based on groups or departments, are these groups audited to make sure it only includes individuals that need access to the data?	By granting data access permission to groups of individuals the administrative processes associated with managing data can be eased, however, if individual membership in different groups are not periodically audited this practice can lead to problems by allowing inappropriate access to data stores.
12.2	Is unauthorized system access attempts monitored and logged?	Unauthorized access attempts, whether reflected by an invalid userid or an invalid password, may be indicators of an hacking attempt. A systematic attempt to break into a system may only become visible by analyzing invalid and validated access attempts over time.
12.3	Do the processes validate the users identity when the log onto the systems by password or some biometric system	It is important to know when a user logs onto and logs off the systems. This information may be important when a data breach is being investigated.
12.4	Are passwords stored as fixed encoding/encrypted strings that might be decoded to discover the password?	If the password file is stolen and then brute force tested, it might be possible to determine the original password or a known password that has been encrypted can be used to deduce the encryption algorithm.
12.5	Is any stored biometric data encrypted and stored in a separate file?	If the password file is stolen and then brute force tested, it might be possible to determine the original password or a known password that has been encrypted can be used to deduce the encryption algorithm.
12.6	Does the organization actively manage encryption by making sure passwords are periodically changed and common or easily guessed passwords are not used?	Many people use common, easy to guess phrases for their password. The system should allow longer pass phrases for passwords and require users to periodically change their passwords.
12.7	Are logs maintained so there is a record of who entered and exited the data centers?	When an investigation is initiated it is often important to have a record of which people were in the data center during the breach.
12.8	During periods of inactivity, are users automatically logged off the system?	When users leave their workstation, if their login remains active others can gain access to the system under a false system identification.
12.9	Are there controls that would prevent data from being exported from protected systems and given to unauthorized users or used for unauthorized purposes?	Email, FTP drives, shared server systems, and other technology makes it easy to share information among users. It also makes it easy to share data that might be intended only for protected use. Systems that allow data to be easily transferred between users' needs to be closely monitored as a point of privacy and security risk.
12.10	Are the staff restricted from downloading and installing unauthorized software to their electronic devices with access to sensitive data?	If an organization allows their ability to download software that has not been properly validated by the security staff, that software may contain malware or features that undermine the organization's privacy conventions. Staff should not be allowed to put unauthorized software on systems that have access to sensitive data or applications.
12.11	Is there a process by which staff can request that unauthorized software be reviewed and considered for future approval? Is there a defined process that any software must undergo before it becomes approved?	When the organization attempts to deny employee access to external software or sites that they consider valuable productivity enhancing tools, it becomes important that the organization provide a path by which employees can request certification of software they believe to be important to them. These requests should be acknowledged and responded to so the employee will know if their request has been denied and why it was refused.
12.12	Is there a defined policy to determine when a site would be blocked or unblocked via the firewall?	The organization should have a list of blocked sites AND they should have a policy statement that describes what sites will be blocked. With a rule in place, it becomes easier for staff to determine if a new site should or should not be blocked from the network.
12.13	Are internet browsers that are used within the secured network, configured to stop web applications from accessing external	Many organizations have systems in place that attempt to thwart efforts to get past system security. To get past these safeguards, malicious users will attempt to embed malware when the systems are connected to the external network and

	sites that might download and run malicious code?	later infect the internal network when that device reconnects behind the firewall.
12.14	Do the operational processes guard against accidental deletion and modification of the data by making sure only authorized personnel can take these actions?	Asking the traditional "Are you sure question" is a step in the right direction but such validating questions can be made more effective by making the question specific to the action requested (e.g. "Are you sure you want to delete/edit record XX")
12.15	Can an operator back out of an erroneous edit or deletion of data through use of back-up systems?	When changes are made erroneously, there should be a record that is sufficient enough to undo the change regardless of whether the error is detected immediately by the operator and many days later by another individual.
12.16	Does the organization's policies describe how and when to pseudo randomize data?	Anonymization of data can reduce the risk to an individual if a breach were to occur but the effectiveness of such measures depends on how data is randomized and when these processes are carried out (earlier being better).
12.17	Does the organization store all sensitive information in an encrypted format?	Encryption algorithm is a generally accepted process for securing data. As standards change, the organization is expected to upgrade their encryption processes.
12.18	Does the system log all application activity from a user so that it is clear what data processes they were using?	An individual user may have access to many applications. Some applications process sensitive data and others may not. It is important for an organization to know when a user is making use of an application that accesses sensitive data.
12.19	Are there auditing processes that review data usage in order to make sure all data usage is properly documented?	Data logs should be available to show who has accessed specific data sets and any changes a specific user may have made to the data set so that process errors can be quickly traced back to their source.
12.20	Is a centralized action register maintained that can be used to ensure that recommended actions to improve privacy/security, regardless of where the recommendation originated from, are tracked through to their conclusion?	It is difficult to manage an organization's cyber readiness if action items are distributed through the organization and not managed in concert from a central staff. Having a centralized action register makes it easier to manage actions to closure and also allows different divisions within the organization to learn from one another
12.21	Is there a public 'hotline' number/email that the general public can use to report potential security issues?	Often, the public (or employees) will notice issues that seem strange like unexpectedly slow performance or apparent website content errors before the organization's staff detects the issue. If the public has a way to report suspicious behavior in the network, these reports can be used as an early-warning threat detection system.
12.22	Is the system architecture constructed as a series of rings that can be isolated from each other in the case of a cyber-attack?	It should be possible to shut off all internet access to the network, shut off internal computer access to the core network, and isolate segments of the core network to prevent detected cyber-attacks further compromising the system.
12.23	Email is a form of data. The email messages, sender, recipient, etc. are all forms of data that need to be tracked like other forms of data. Does the email policy adhere to the data privacy guidelines?	Email policies should indicate when email is to be purged, email logs should be secured, and the content and email meta-data should be protected.
12.24	Are internal FTP and file exchange services completely disabled from external access?	External sources should not be able to deliver files or retrieve files from the organization's internal network.
12.25	Do email systems block attachment of larger files?	Large files attached to emails should be treated suspiciously.
12.26	Are all incoming e-mail attachments scanned for viruses?	Viruses are often included in files attached to emails.
12.27	When larger files must be transferred out of an organization an external intermediate party should be used to facilitate the exchange and that party should scan all transferred files (both in and out) for viruses.	Use of a third independent party provides an intermediate layer of external protection to minimize the potential for corrupted files making it into the organization's internal network. All files on the external site should be stored in an encrypted format.
12.28	Are files exchanged on a file exchange service encrypted by default with access limited to those with an explicit invitation for access?	The file exchange system should not be used to distribute publicly accessible files. Public files are better served from a separate but publicly accessible server.
12.29	Are the organization's externally visible website files stored on the same network as the organization uses for internal communications?	The publicly visible website files should be stored on an external server so that if a hacker corrupts the website, they do not have the potential to corrupt the organization's internal network.

INDUSTRY SPECIFIC ISSUES

Some privacy/security issues can be considered as being specific to certain industries. These issues often become generalized and thus the industry specific privacy/security issues can be expanded to include other industries over time. In addition, customers and partners who operate across industries often begin to expect the treatments they receive through one relationship become expectations of other industries. As a result, while these issues may not immediately apply outside that industry, people should be aware of the issue and consider creating an analogous policy for their organization in order to prepare for future requirements.

13.1	If the organization maintains credit information on customers, does the organization automatically notify the user when a third party asks for information to process a transaction, collect a debt, or validate credit history about a user's credit?	If the organization holds credit related information and shares that information with third parties, they should notify end users if a third party requests credit information so the individual will know when data about them is being accessed
13.2	If the organization obtains and uses credit information in order to transact business with their customers, does their data policy prevent them from holding personal information provided by credit card companies after the transaction has been completed?	When companies interact with consumers they may need to interact with credit companies to complete a transaction. Companies should not hold this data for other possible uses - the data should be deleted immediately after the transaction is complete.
13.3	If an organization releases employee data to insurance companies or other third parties that support the organization, are the employees aware of the data release and are there legal safeguards in place to make sure they guard employee privacy?	Some companies (e.g. health insurance companies), have a legitimate need to know about the employees they are insuring when they provide health coverage for an organization. In these situations, the employee should provide consent or the policy describing what specific information will be shared with identified third parties should be well documented.
13.4	If the organization is a healthcare organization, do they ask for consent before disclosing healthcare Information to third parties?	If the organization is a healthcare organization, they can disclose protected health Information if it is necessary to carry out treatment, payment, and health care operations but when they do so, the organization should provide individuals with a report that describes the disclosures and the third parties that have had access to this data?
13.5	Has the organization joined the EU-US Privacy Shield Program which allows the organization to self-certify compliance with EU privacy laws with the US Dept. of Commerce?	Organizations must have a suitable data privacy policy statement, a defined process to investigate complaints, agree to submit to binding arbitration to resolve issues, and an assigned privacy officer to oversee complaint responses.

FACIAL RECOGNITION, AUDIO DETECTION, VIDEO ANALYTICS

As a new technology is introduced to the IT systems, each new technology should be carefully considered for implications related to security and privacy. Deployment operational standards and their implications can be considered. People often become fearful of new technologies when their use is not governed and there is the potential for improper use.

14.1	If facial recognition is used, have standards been established to govern how, where, and when the technology can be used?	Before the organization deploys facial recognition, the organization should have clear standards that determine where, when, and how the technology can be used within the organization.
14.2	If facial recognition is used, are there rules about how the data is obtained?	Facial recognition technology is driven by image data. There should be clear rules about how the data that is used by the technology is used, where imaging devices may be placed, and when that data will be deleted.
14.3	If facial recognition is used, is it clearly posted in areas where the technology is used?	When facial recognition is being used, the fact that the technology is in use should be clearly posted.
14.4	If facial recognition is used to link an image with a name, has the named user given permission to make that association?	Facial recognition technology scans an image and compares that image with a database of known images. If the known image is associated with a person, the person should have the ability to validate that linkage.
14.5	Is the raw imaging data used by the facial recognition system covered by extremely strict privacy and protection rules?	Facial recognition starts with raw video files, scans for faces, and attempts to match the scanned images with a library of known people. The library of images is especially sensitive and should be guarded carefully. Also, any captured video is also especially sensitive and special handling is warranted and should be detailed.
14.6	If voice recognition is used, have standards been established to govern how, where, and when the technology can be used?	Before the organization deploys voice recognition, the organization should have clear standards that determine where, when, and how the technology can be used within the organization.
14.7	If voice recognition is used, are there rules about how the data is obtained?	Voice recognition technology is driven by audio data. There should be clear rules about how the data that is used by the technology is used, where audio collection devices may be placed, and when that data will be deleted.
14.8	If voice recognition is used, is it clearly posted in areas where the technology is used?	When voice recognition is being used, the fact that the technology is in use should be clearly posted.
14.9	Does the raw audio data used by the voice recognition system face extremely strict privacy and protection rules?	Voice recognition starts with raw audio files, scans for command indicators, and attempts to take action or collect data based on detected commands. The data collected from these systems may be sensitive and should be guarded carefully. Also, any captured audio should be treated as sensitive data that could be scanned for other purposes in an unsecured environment.
14.10	If the organization collects audio data, does the privacy policy describe what can and what cannot be done with the audio files	If the digital data is derived from audio data, the policies that guide use (and misuse) of digital data should be applied to the audio data as well meaning that the owners of the audio data collection system should be notified that their devices are being used to collect audio data that will be digitized for specific purposes
14.11	If the organization uses audio files to analyze their content, is the data derived from the audio treated as user data and subjected to the same controls as other customer/partner data?	The policies that guide the use of digital data derived from audio data should be applied to the derived digital data based on the source of the source audio data records.
14.12	If the organization collects audio data, is the data logged by source user, date, and location of collection?	If audio data is used to create digital data, it is important that there be meta data that source the digital data back to the originating audio data and that the audio data is identified by the source of the data (ownership of the collecting device).