[COMPANY] Compliance, Security, Classification, Data Governance and Risk Management Policy

An [COMPANY] Corporate Guide

THIS [COMPANY] COMPLIANCE, SECURITY, CLASSIFICATION, DATA GOVERNANCE AND RISK POLICY DOCUMENT COVERS ALL STEPS REQUIRED FOR TRACKING AND IMPLEMENTING OUR TANGIBLE AND INTANGIBLE INVENTORY NOW WITH FRAMEWORK FOR FUTURE GROWTH.

Table Of Contents

Purpose

Best practices for security, classification, governance, and risk management policies are defined to minimize risk, ensure compliance, build trust, and protect the [COMPANY] brand.

A risk and compliance management strategy is an ongoing process and not a one-off activity. The following is a good first step in developing the processes[1]:

- ❏ Carry out Gap Analysis by Policy owners
- ❏ Map requirements (requirements will be set by the different stakeholders/executives) , create a checklist and identify any discrepancies
- ❏ Get top-level buy-in
- ❏ Assign a senior manager with responsibility for security, and data steward(s)
- ❏ Create the role of Security Administrator
- ❏ Establish security and data policies that are compatible with existing Federal, Corporate, and IT Policies

[1] Many of these steps, such as defining a Security Administer, are to be done after the company reaches the next maturity level. This condition applies as needed, to other processes defined in this document.

❏ Define data security levels such as Sensitive, Confidential, Private, Proprietary, and Public
❏ Identify Users, Roles and Data Accesses privileges
❏ Define Key Risk Indicators (KRI)
❏ Monitor KRI with dashboards to continuously display results

Monitoring

There are defined processes following industry standard enforcement to monitor operational situations and apply the required precautions. When a Security Administrator is on board, security will create a set of key risk indicators (KRIs), backed up by the voluminous data an information the security team collects.

Currently COO (**MIchal)** for business for impact purposes develop monitoring system. Eng Head (**Erez Ops**) for db, servers, etc. develop monitoring system using KRIs.

Data Security Architecture

This Architecture shows three distinct levels of data security architecture: Governance, Risk and Compliance (GRC).

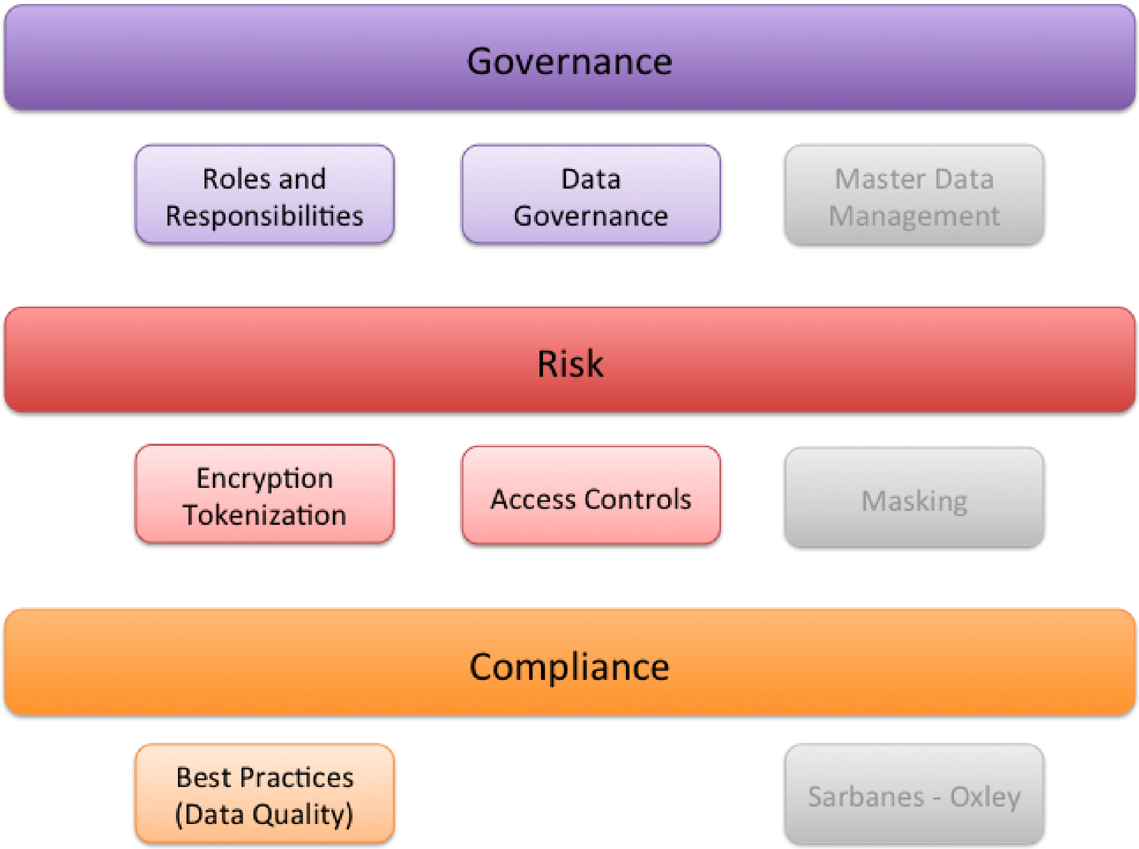


Figure 1: Three levels of data security architecture: Governance, Risk, and Compliance

This policy addresses GCR specifically after defining the [COMPANY] Security Policy and Data Classification sections.

Security Policy

There are defined security policies for each data class, candidates and companies, financial, and reports following industry standards.

To facilitate this policy, we will use external companies who check for security problems, such as Altoros, KPI Partners, LatentView Analytics, CBIG Consulting, or Denologix. See https://clutch.co/it-services/analytics/leaders-matrix for further discussion on best external security advisors advisors.

Inventory Assets Tracking

This section is about current inventories of IT assets, such as hardware, network devices, and existing inventories, that should indicate sensitivity, critical items, assets, and any sensitive data stored on it matched to the inventories. This live and adjustable tangible “Assets Tracking” spreadsheet is the asset inventory which naturally changes over time.

Every tangible asset that cost over $1,000 and was bought by the company, or bought by an employee and got reimbursed by the company gets a tracking sticker with a running number. The office manager records the asset and tags it with the sticker. The office manager manages a detailed list of all Company assets, their tagging number and their current position the (‘Asset Tracking List’). Finance keeps a list of the assets, their original cost and their depreciation in the company's accounting system (‘Accounting Asset List’) . Finance reconciles between The Asset Tracking List and the Accounting Asset List on a quarterly basis. Finance and the office manager have access to the Asset Tracking List.

Information assets are handled according to how critical and sensitive they are. The rules for acceptable use of information assets are documented and implemented.

Network

Network security policies for [COMPANY] networks are:

- ❑ firewall
- ❑ passwords
- ❑ SSH keys - for private and public networks
- ❑ access control
- ❑ data loss prevention

- ❏ inbound and outbound email
- ❏ WIFI
- ❏ Office network

There are rules to be implemented that defines a method preventing unauthorised people from accessing sensitive areas, such as plugging into the wired network.

Code

Code review minimizes security risks, as design and code inspections reduce far greater defect detection than QA. There are rules to be implemented as to who reviews and approves:

- ❏ [COMPANY] back-end code
- ❏ Open Source
- ❏ Third party code for security issues[2]

Rules For Acceptable Use Of Information Assets

Preserving the integrity and consistency of [COMPANY] data is defined in this section.

One metric users cause to make decisions is based on our high-quality data and well-managed information assets, We employ effective information assets use and governance set by for data management and usage parameters and processes to resolve data issues.

Data security processes and permissions are yet to be fully implemented. User Profiles should be the first one to be addresses, such as forbidding exporting real names and associated data. Exceptions can be defined later, such as executive levels and above.

Governance

Governance, Risk and Compliance (GRC) business policies, software solutions and services enable [COMPANY] to implement, manage, monitor, and measure the effectiveness of these strategies. GRC strategies rely on clearly defined, objective measurables for providing companies with insight into the overall effectiveness in each area of governance, risk and compliance.

Data Governance

In this section, data governance is defined as an organizational approach to data and information management that is formalized as a set of policies and procedures encompassing the full life cycle of data, from acquisition to use to disposal. A proper governance process manages data projects and stops including misleading data and unexpected costs.

[2] Reference https://info.veracode.com/state-of-software-security-report.html

Data governance requires discovery, definition and documentation phases with discussions and meetings so that Business and IT achieve a common and holistic understanding of what data is used and how it is used to make business decisions. Definitions must be accepted or used by the business. Plans must match expectations.

To that end, [COMPANY] uses cloud best data governance practices assuring compliance for data that is traveling in and out of clouds by implementing:

- ❏ Automation
- ❏ DevOps
- ❏ Agile programming
- ❏ Continuous Deployment

[COMPANY] follows data and information management audit guidelines for certification and regulatory compliances by maintaining the following:

- ❏ Network architecture configuration and access control features only allow critical employee access to data, external APIs, and FTP server control.
- ❏ Encrypting all traffic from an external browser. Internal traffic is secure and is not encrypted.
- ❏ Audit logs.
- ❏ User authentication across system components including audit logs.

In this way, [COMPANY] meets the industry best practices in accordance to the level of corporate development. As the business grows, [COMPANY] will update processes, ensuring that all the data is logged, authenticated and meets audit standards.[3]

[3] When the data is being used in non-production environment, the PII data must be scrubbed.

Roles and Responsibility

Each [COMPANY] employee have defined roles with respect to each data class, so that admin, engineer, and others have predefined rules with exceptions regarding the master data. And reviewing 3rd party data rule with processes and checklists.

- ❏ Admin: Minimum of two people have access to everything. Titles are at manager level.
- ❏ Engineer: R/W access to all except user accounts
- ❏ Others: R to all

PRODUCTION ENV.	Marketplace	External	Financial	Reports	Analytics	Misc
Admin	RW	RW	RW	RW	RW	RW
Eng	RW	R	-	R	R	RW
Data Scientist	R	R	-	R	RW	RW
Biz Op	R	R	-	RW	R	R
Finance	R	R	RW	R	R	R

Note: In the future, engineers can have temporary RW to any system.

Acceptance qualifications for external data class are:

- ❏ Reviewed by at least one Product Team member
- ❏ Reviewed by at least one Data Science team member
- ❏ Reviewed by at least one Engineering team member
- ❏ (*If there is a financial impact)* Reviewed by at least one Finance team member
- ❏ (*If there is a security impact)* Reviewed by at least one Security expert
- ❏ Reviewed by at least one Legal team member

Each employee must have a unique username & password for accountability.

All data is contained in completely isolated environment which is not accessible from the internet.

Data Compliance and Classification

There are different classes of data in our main database - the candidates and companies (two sides of the marketplace), customers, internal financial data, and reports. The behavior, monitoring, and risk is different for each class of data. Data from external sources, such as Crunchbase, Synthio, and O*Net, which are used in the matching algorithm.This section looks at the data life cycle, main data, financial data, and reports each with respect to governance, risk and compliance.

Data Life Cycle Management

Data lifecycle management compliance practices are defined to diminish risks of data loss, deletion and breaches, as well as the fines, penalties and downtime.

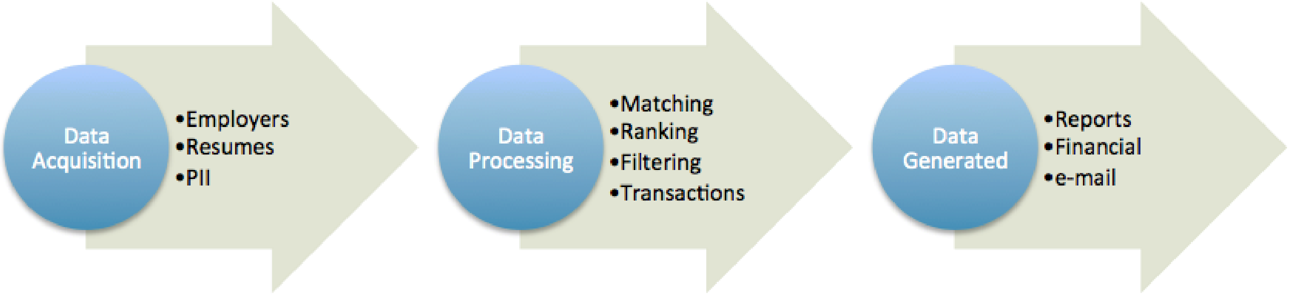


Figure 2: Data stewardship for acquisition, processing, and generation

The following is a broad checklist for handling all data types. [COMPANY] has and updates the following measures:

❏ Define data types
❏ Strong data backup plan
❏ Archive outdated third-party data and models (such as AI related databases)
❏ Set data deletion guidelines to industry guidelines. We do not delete data.
❏ Define a data governance policy

By implementing management practices, [COMPANY] data stays secure throughout the data lifecycle.

Backup

[COMPANY] compliance practices are creating full backups and daily storage snapshots on non-production systems with the following procedures:

❏ Snapshots of marketplace, financial, and miscellaneous data are kept for 30 days.
❏ Data backups in database-specific formats are retained and protected at all times.
❏ Active-active real time replication of reports with at least two synchronous copies of the application database.

Marketplace Data Class

Marketplace data class includes the information entered to the product by the marketplace user of the following types:

- ❏ Job seekers
- ❏ Recruiters
- ❏ Employers

This information include details regarding job positions, position requirements, work history, job preferences etc. This data includes also sensitive PII (Personal Identification Information) such as names, phone numbers, addresses and email addresses.

When the data is being used in non-production environment, the PII data must be scrubbed.

External Databases Data Class

The External Data Class stores data from external databases which includes information regarding professionals and employers. We obtain data from several external databases such as Synthio, Crunchbase, O*Net.

Financial Data Class

This section refers to any money related information. The Financial Information Class stores any other financial documents, such as agreement terms with the company’s customers pricing, payment, and credit terms. This class provides a safe and secure information location for quantity and dollar amounts in all of [COMPANY] financial transactions.

There are two financial data sources:

- ❏ static information
- ❏ transactions

Items stored here are:

- ❏ Agreement terms
- ❏ Credits
- ❏ Payments
- ❏ Invoices
- ❏ Discounts
- ❏ Reports with money line items
- ❏ Any other financial paperwork or dealings

This is highly secure so that there are no reproductions of this data class and minimal number of employees with full access.

Reports Data Class

The Reports Data Class includes operational data. Operational data regarding marketplace users and their matching. Conversion Report to monitor. Reports Data Calls never contains reports that include monetary dealings.

Analytics Data Class

Analytics Data Class is an internal data class for data such as research and development data or mixpanel data.

Miscellaneous Data Class

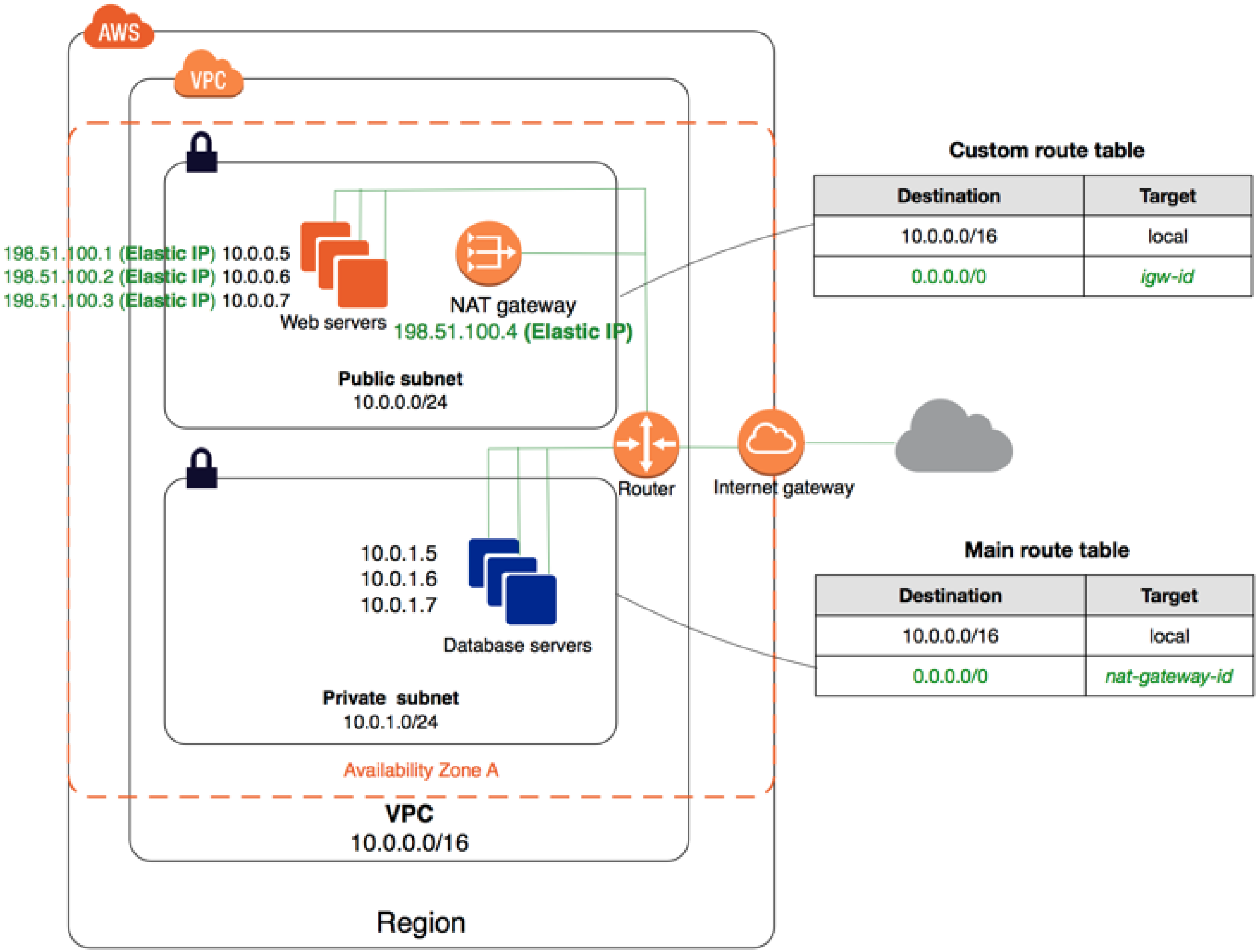
Miscellaneous Data Class includes information that the products' models use for matching, ranking and filtering and are not classified as other data classes. This includes lists of countries, lists of job titles, zip codes etc. This sort of information is generally not considered sensitive and is not proprietary of the Company.

Risk

The level of reward to risk is at a moderately low at this point for a high security policy against hackers. All engineers have access to data. Access is controlled with SSH keys per user/engineer. When an engineer leaves, someone has to go to every machine that had access to the [COMPANY] network they and remove the public keys of each ex-employee. We will need to move to a different configuration, in which, only two machines are connected to the public network and and other machines are connected to the private network, and you can reach them only through these two machines. Therefore, when we want to disconnect an ex-employee from the public network, we need to work only on three machines.

Under normal circumstances, data should not be copied to personal laptops, so that data does not leave company property.

We need a solution to add with the correct permissions and remove access from all people that leave the company. The following network architecture diagram is recommended, popular solution suggested by AWS, with easily configurable access control.



Custom route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

Figure: [COMPANY] Amazon Virtual Private Cloud public and private subnet configuration based on AWS best practices

Encryption

Data on the production system is not encrypted. If data is copied to corporate mobile devices, such as a laptop, the disk, and taken outside the company offices must be encrypted. All laptops that are downloading any part of any [COMPANY] databases must have encryption enabled.

Application Access Control

Application access control must be in front of all internet-facing services[4]. There are two steps to control access:

1. **Authenticatication**; the remote system verifies the user. A common technique is to use cookies.
2. **Authorization**; the system checks the user permissions to allow and block access based on those permissions.

Compliance and Data Quality

Data governance is a continuous quality improvement process to filter bad information by defining and enforcing policies and approval procedures for achieving and maintaining data quality. It defines a data management strategy with business users taking ownership of preserving the quality of the data.

The following are best practices [COMPANY] follows Data Classification and Compliance involving data quality and business user initiatives:

❏ As a baseline and periodic check, perform an analysis of the current state of the data sets and security, such as API access, encryption, and access controls.
❏ (AWS feature) Use a quality firewall detects and blocks bad data at the point it enters the environment, acting to proactively prevent bad data from polluting enterprise information sources.
❏ Identify and prioritize types and volume of data that requires data governance for quality management and governance.
❏ Appoint one or more data stewards as watchers over data integrity issues end-to-end. They act as liaisons with the IT group managing underlying information management infrastructure. For example, the data architect would be responsible and adjust the policies as the business changes.
❏ Business users to take ownership per data class they are helping to create and feeding into the database. For example, the CFO is responsible for the Financial Data who creates and enforces the policies. See the internal RACI document.

Data Integrity Teams

Successful data governance starts with a solid, well-defined data management strategy, and relies upon the selection and implementation of a cutting edge data quality management solution. The key to effective data quality management is creating data integrity teams, comprised of a combination of IT staff and business users, with business users taking the lead and maintaining primary ownership for preserving the quality of any incoming data.

[4] See https://kemptechnologies.com/white-papers/securing-internet-facing-applications/ for current thoughts.

While data integrity teams drive the data quality management plan forward, it is also important to have a comprehensive data quality management solution in place. This makes the strategy more effective by enabling data governance professionals to profile, transform and standardize information.

Safe Open Source Integration

Engineering must do research and get approval from the Open Source authority manager when checking Open Source code against our compliance levels. In particular, there are some open sources that have very strict licenses which need to be verified and reviewed to predict impact on:

- ❏ Size
- ❏ Stability
- ❏ Cost
- ❏ Security
- ❏ Scale

Many of license requirements resources are collated under The Linux Foundation's Open Compliance Program.

Summary

[COMPANY] understands good governance is an ongoing framework that expands to stay in concert with the growth of the company and the tangible and intangible Intellectual Property and database it implements a data governance framework by following current industry standards such as:

- defining data ownership questions
- data inconsistencies across different departments
- enforcing rules when:
  - expanding the database collection
  - when using big data in companies

Because GRC strategies span the entire organization, these tools and policies require management and coordination across the entire company, including IT, management and legal departments.

Post Note

This policy is written prior to [COMPANY] retaining clients. Therefore it does not have the risk level or staff to warrant full implementation of processes and procedures defined in this policy. Many of the solutions, key triggers, and teams described here, will be implemented in the future when the company assets demand support using this infrastructure.

Appendix A

Checklist for Data Governance Standard Policies and Procedures

The purpose of this checklist is to assist stakeholders with establishing and maintaining a successful data governance program as the [COMPANY] databases grows.

An approach to data and information management is a formalized set of policies and procedures for the full life cycle of data, from acquisition to use to disposal. This includes establishing decision-making authority, policies, procedures, and standards regarding data security and privacy protection, data inventories, content and records management, data quality control, data access, data security and risk management, data sharing and dissemination, as well as ongoing compliance monitoring of all the above-mentioned activities.

Decision-making authority

Assigning appropriate levels of authority to data stewards and proactively defining the scope and limitations of that authority is a prerequisite to successful data management.

- ❏ Has an organizational structure with different levels of data governance such as executive, and administrative rights have been established, and roles and responsibilities at various level specified, such as technology leaders and data stewards?
- ❏ Have data stewards responsible for coordinating data governance activities identified and assigned to each specific domain of activity?
- ❏ Are data stewards' roles, responsibilities, and accountability for data decision making, management, and security been clearly defined and communicated to data stewards themselves as well as stakeholders?
- ❏ Do data stewards possess the authority to quickly and efficiently correct data problems while still ensuring that their access to personally identifiable information (PII) is minimized in order to protect privacy and confidentiality?

Standard policies and procedures

Adopting and enforcing clear policies and procedures in a **written data stewardship plan** is necessary to ensure that everyone in the organization understands the importance of data quality and security—and that staff are motivated and empowered to implement data governance.

- ❏ Identify policy priorities affecting key data governance rules and requirements and have key stakeholders agreement on those priorities.
- ❏ Have standard policies and procedures for data governance and the data management lifecycle, including collection, maintenance, usage and dissemination clearly defined and documented?

- ❏ Are policies and procedures in place that ensure all data are collected, managed, stored, transmitted, used, reported, and destroyed in a way that preserves privacy and ensures confidentiality and security?
- ❏ Has an assessment been conducted to ensure the long-term sustainability of the proposed or established data governance policies and procedures, including adequate staffing, tools, technologies, and resources?
- ❏ Is there a written plan for monitoring compliance with established policies and procedures?
- ❏ Have data governance policies and procedures been documented and communicated in an open and accessible way to all stakeholders, including staff, data providers, and the public (e.g., by posting them on the organization's website).

Data inventories

- ❏ Conducting an inventory of all data that require protection is a critical step for data security projects.
- ❏ Maintaining an up-to-date inventory of all sensitive records and data systems, including those used to store and process data, enables the organization to target its data security and management efforts.
- ❏ Classifying data by sensitivity helps the data management team recognize where to focus security efforts.
- ❏ Does the organization have a current inventory of all computer equipment, software, and data files.
- ❏ Does the organization have a detailed, up-to-date inventory of all data elements that should be classified as sensitive (i.e., data that carry the risk for harm from an unauthorized or inadvertent disclosure), PII, or both.
- ❏ Have data records been classified according to the level of risk for disclosure of PII.
- ❏ Does the organization have a written policy regarding data inventories that outlines what should be included in an inventory and how, when, how often, and by whom it should be updated.

Data content management

Closely managing data content, including **why and which data are collected**, is necessary to justify the collection of sensitive data, optimize data management processes, and ensure compliance with federal, state, and local regulations.

- ❏ Does the organization have a clearly documented set of policy, operational, and research needs that justify the collection of specific data elements (e.g., what PII needs to be collected to successfully monitor participation in and progress through the system).
- ❏ Does the organization regularly review and revise its data content management policies to assure that only those data necessary for meeting the needs described above are collected and/or maintained.

Data records management

Specifying appropriate managerial and user activities related to **using and handling data i**s necessary to provide data stewards **a**nd users with appropriate tools for complying with an organization's security policies.

- ❏ Have mechanisms been put in place to de-identify PII data whenever possible (e.g., by removing all direct and indirect identifiers from PII).
- ❏ Has the organization established and communicated policies and procedures for handling records throughout all stages of the data lifecycle, including acquiring, maintaining, using, and archiving or destroying data.

Data quality

Ensuring that data are accurate, relevant, timely, and complete for the purposes they are intended to be used is a high priority issue for any organization. The key to maintaining high quality data is a proactive approach to data governance that requires establishing and regularly updating strategies for preventing, detecting, and correcting errors and misuses of data.

- ❏ Does the organization have policies and procedures in place to ensure that data are accurate, complete, timely, and relevant to stakeholder needs.
- ❏ Does the organization conduct regular data quality audits to ensure that its strategies for enforcing quality control are up-to-date and that any corrective measures undertaken in the past have been successful in improving data quality.

Data access

Defining and assigning differentiated levels of data access to individuals based on their roles and responsibilities in the organization is critical to preventing unauthorized access and minimizing the risk of data breaches.

- ❏ Are there policies and procedures in place to restrict and monitor staff data access, limiting what data can be accessed by whom, including assigning differentiated levels of access based on job descriptions and responsibilities.
- ❏ Are these policies and procedures consistent with applicable local, state, and federal privacy laws and regulations.
- ❏ Have internal procedural controls been established to manage user data access, including security screenings, training, and confidentiality agreements required for staff with PII access privileges.
- ❏ Are there policies and procedures in place to restrict and monitor data access of authorized users (e.g., researchers) to ensure the conditions of their access to data in the system are consistent with those outlined in the data governance plan, including which data elements can be accessed, for what period of time, and under what conditions.

Data security and risk management

Ensuring the security of sensitive and personally identifiable data and mitigating the risks of unauthorized disclosure of these data is a top priority for an effective data governance plan.

- ❏ Has a comprehensive security framework been developed, including administrative, physical, and technical procedures for addressing data security issues (such as data access and sharing restrictions, strong password management, regular staff screening and training, etc.).
- ❏ Has a risk assessment been undertaken, including an evaluation of risks and vulnerabilities related to both intentional misuse of data by malicious individuals (e.g., hackers) and inadvertent disclosure by authorized users.
- ❏ Is a plan in place to mitigate the risks associated with intentional and inadvertent data breaches.
- ❏ Does the organization regularly monitor or audit data security.
- ❏ Have policies and procedures been established to ensure the continuity of data services in an event of a data breach, loss, or other disaster (this includes a disaster recovery plan).
- ❏ Are policies in place to guide decisions about data exchanges and reporting, including sharing data (either in the form of individual records containing PII or as de-identified aggregate reports) with educational institutions, researchers, policymakers, parents, and third-party contractors.
- ❏ Are stakeholders, including customers and job seekers, regularly notified about their rights under applicable federal and state laws governing data privacy.

Glossary of Security Terms

Refer to the SANS online Glossary of Security Terms list, https://www.sans.org/security-resources/glossary-of-terms/