Information Security Policy (ISP) Standard

Network Data Classification Standard

Version 1.01

Data Classification:
***Internal** Use Only*

January 2018

pwc

Table of Contents

Document History

Version	Date	Changes Made	Author(s)
1.00	June 2017	Initial Publication	Joe Frisk
1.01	January 2018	Adjustments to align with NDPP requirements	Joe Frisk

References to Additional Standards, Procedures, Guidance		Reference
1	Network Information Security Policy	**Spark Page**

Scope

The Information Security Data Classification Standard applies to all PwC member firms for all information and systems.

It is the policy of the PwC network that the information assets of the member firms be protected from internal or external threats, whether deliberate or accidental, such that:

- Data subject rights are respected.
- Confidentiality of information is maintained.
- Integrity of information can be relied upon.
- Information is available when the business needs it.
- Relevant statutory, regulatory, and contractual obligations are met.
- The PwC brand is protected.

Firm personnel must protect information assets from all types of threats and ensure the confidentiality, integrity, and availability of information and technology assets.

Disclaimer

The information contained in this statement is for Internal Use only and should not be distributed further without written consent from PwC Network Information Security.

Intent

The PwC Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a technical standard and control capability throughout PwC and its member firms to help protect PwC from unauthorised access to confidential data.

PwC demonstrates its commitment to IT security through the implementation of policies, controls and standards. All PwC territories are responsible for complying with PwC's ISP. In some instances additional policies are required based on client, regulatory, internal audit, and other identified risk drivers.

Policy Standard

PricewaterhouseCoopers ("PwC") and its leadership take the security of PwC's information, infrastructure and applications seriously. The confidentiality, integrity, and availability of information and information systems is critical to the uninterrupted operations and timely provision of services. PwC gathers and generates large amounts of data with varying levels of sensitivity to support its business activities. As a result data is processed, transmitted and stored by information systems and individuals.

The identification and categorization of Firm and Firm client data is necessary to understand where sensitive data resides and any additional review of data collected, created, stored, and transmitted across the environment to protect throughout its lifecycle.

The loss or breach of data can adversely impact the individuals referred to in that data, Firm operations, services and reputation, and may result in financial penalty and loss of contracts.

Application owners and project sponsor must define any personal data along with the purpose for storing or processing within an application or system in the formal application inventory as required per the Network Information Security Policy. Client engagement teams must define any personal data along with the purpose for storing or processing personal data within client engagement activity.

Applications, systems and client engagement teams must maintain and track source of personal data and be familiar with the process to update or delete from the system of record where requested.

The purpose of this document is to establish the Data Classification Framework (DCF) and provide Firm personnel with guidance around assigning a level of sensitivity to assets and the secure management of data (paper and electronic) from unauthorized access, use, modification, and disclosure. This document is a management approved companion to the ISP and includes controls that either augment an existing ISP control, or add an additional control.

Member Firms must adopt the centralised NIS data classification service.

Data Classification Framework

The PwC data classification framework is based on the data value and sensitivity. Proper classification considers the potential impact on an individual or PwC with the loss of confidentiality, integrity or availability in the event of a security breach.

Confidentiality is preserving authorised access and disclosure of information and the potential impact to the organisation, operations or an individual.

Integrity is protecting against improper use of information (e.g. modification, destruction) where unauthorised activity would create potential impact to the organisation, operations or an individual.

Availability is to ensure reliable and timely access to information to conduct business activities and the disruption of access would have impact to the organisation, operations or an individual.

To achieve and maintain appropriate accountability, protection, and use of Firm data, all data must be classified according to its sensitivity and criticality.

Sensitivity measures the control of access to data while criticality measures the importance of the data to the organization. When determining the sensitivity of data, a key component is looking at the relevant compliance, legal and contractual requirements as mandated by laws, regulations, and standards.

Criticality of data is determined based on its importance or risk relative to Firm goals and objectives, including the uninterrupted operation of essential business and IT functions. Typically, requirements around availability and integrity drive the criticality level of the data.

Typically, requirements around confidentiality drive the sensitivity level of the data.

The following classification scheme detailed in the table below outlines the classification levels and provides a basis for understanding and managing of information assets:

Classification Label	Definition	Potential Disclosure Impact
Public	Information that is intended for public use. Disclosure would not negatively impact PwC.	No negative impact or implications if disclosed or lost.
Internal	Information intended for internal use by PwC partners and staff. Unauthorised external disclosure will cause minor damage to PwC.	Unauthorized disclosure or loss may cause **embarrassment** to PwC, involve minor damage to the PwC brand and reputation, and/or result in minor financial loss or penalties.
	Additional "**restricted**" attribute can be assigned to	Unauthorized disclosure or loss may be in breach of PwC's legal

	identify data with additional restrictions based on country or regional regulatory requirements.	responsibilities and result in **penalties**.
Confidential	Information subject to a need-to-know basis for certain individuals or groups.	Unauthorized disclosure or loss may cause **significant** damage to the PwC brand and reputation, be in breach of PwC's professional, contractual or legal responsibilities and/or result in significant financial penalties.
	Additional "**restricted**" attribute can be assigned to identify data with additional restrictions based on country or regional regulatory requirements.	Unauthorized disclosure or loss may be in breach of PwC's legal responsibilities and result in **significant** financial penalties.
Highly Confidential **(e.g. Higher Government Classification)**	Information for which unauthorised disclosure will cause major damage to PwC.	Unauthorized disclosure or loss may cause **severe** damage to the PwC brand and reputation, be in breach of PwC's professional, contractual or legal responsibilities and/or result in severe financial and regulatory penalties.
	Additional "**restricted**" attribute can be assigned to identify data with additional restrictions based on country or regional regulatory requirements.	Unauthorized disclosure or loss may be in breach of PwC's legal responsibilities and result in **severe** financial and regulatory penalties.

Regulated data is categorised as "restricted" by PwC as information that requires a greater level of protection due to the nature of the information and the potential consequences should that information be compromised.

The table below further illustrates how data should be classified with examples of each data classification. Additional personal data categories are available with the network data protection program aligned with EU regulations. (*NDPP - Personal Data Fields and Categories*)

Classification	PwC Data	Personal Data (PII)	Entity Data (e.g. client, supplier)

Public	• Website content
	• Marketing materials
	• Newsletters generated for public use
	• Publically available content on social media or other online channels (e.g. LinkedIn, YouTube, Facebook)
	  • Name
	  • Employer
	  • Work address
	  • Work email address
	  • Work phone number
	*Despite this Public classification, there may be additional handling requirements for the above data types.
		Not Applicable as personal data should be dealt with as part of a higher data classification.	• Publicly available information about client or suppliers

Internal	• PwC office or administrative internal communications (e.g. relocation, office specific, newsletters) • Website subscription content • Reference and training materials • Policies, standards, procedures, methodologies, templates	**Partner and Staff information**: • Partner and staff directories (email, phone, etc.) • Business card information (name, title, email, employing firm, office address and office phone)	• PwC client numbers [identifying numbers for clients] • Employer Identification Number (EIN) • General business information that refers to clients [e.g. information in Source,

	• Organisational charts • Event and PwC member firm calendars • Internal project level financial and resource data • Revenue and other PwC financial data prepared for client distribution. (e.g. Global Annual Review) • News and research information provided through subscription services • Production network designs and internal hardware device IP addresses	• Employee identification (GUID, application/system login ID, employee ID) • Class level • Employment status • Anonymised bulk data (all sensitive elements removed or obfuscated) ulilised for analysis or testing • Employee photograph **Client information** • Business card information (name, title, email, employer, office address and office phone)	information in financial systems] • Redacted and anonymised proposal templates or sample work deliverables (i.e. no client identifying information and no client proprietary information)
Confidential	• Internal communications intended for specific individuals or a known limited group. (e.g. client engagement team information sharing) Information about PwC business activities, including: • Strategy • Human resources (planning, mobility, etc.) • Public Relations, communications and government relations (institutional / external relations	**All information** • Any Social Media (Facebook, LinkedIn) personal data content available to only those people who are personal connections • Geo-location • Resumes/CVs • Age/Date of Birth • Veteran status • Languages spoken • Password or PIN number (separate from the user ID) for an individual that	**Confidential data - General** • Confidential client files • Proposals (*engagement client contract terms and sensitivity may drive additional handling requirements) • Deliverables • Work papers • Supporting documentation for work papers (e.g. emails,

	• Finance and treasury (e.g. member firm financial results, margins, inter-firm billing rates, realisation rates, financing agreements, insurance policies, accounts receivable and payable)
	• Marketing and Sales information (including CRM data, targets, feedback on losses, client feedback)
	• Procurement and supplier information (e.g. non-disclosure agreements, proposals, request for proposal responses and vendor scoring).
	• Joint business relationships (agreements, etc.)
	• General M&A activity work
	• Independence consultations
	• General OGC files
	• Advice memos,
	• Attorney-client privileged Communications and Advice on routine matters
	• Filed briefs
	• Risk & Quality output files; (e.g. acceptance and continuance, anti-money laundering findings, quality reviews, consultations)
		controls access to a PwC information or a hardware asset
		• Gender (e.g. Male, Female) / marital status
		
		Partner and staff information
		General
		• Staff personnel records
		  • Performance evaluations, ratings and development plans
		  • CPE and training records, learning records and transcripts
		  • Employment agreement
		  • Job history / education
		  • Compensation and Financial Data (e.g. Salary, bonus, tax returns, retirement benefits, investments)
		  • Class levels and promotion history
		  • Benefits
		  • Home address
		  • Emergency contact information, next of kin and beneficiaries
		• Payroll
		• Independence system information (e.g. holdings, disposal)
			information submitted by client, etc.)
			  • Policies and procedures
			  • Intellectual property
			  • Strategy documents
			  • General financial statements/information
			  • Trial Balance
			  • Engagement contracts
			• Client financial transaction data and financial holdings data for individuals
			• Individual and Corporate Tax Returns
			• Other confidential information received from PwC clients or other parties with whom we do business
			
			{Restricted}
			• Data of government clients or other data that is designated as sensitive from a national security standpoint under relevant local law (e.g., China State Secrets, US government data, etc.) ** Note special handling requirements will often apply to such data,

	• Security incidents or security vulnerability information	• Annual Compliance Confirmation **Client information** • CRM data regarding client and potential client contacts **Supplier Information** • Confidential vendor proposals, tenders, quotations • Contracts	including, for example, restrictions on data export and on handling of data by foreign nationals.

Highly Confidential	• Network documents
	  • Regulations
	  • Network Standards
	  • Firm Services Agreement
	• Certain OGC files:
	  • Litigation strategy
	  • Insurance reserves
	  • Internal investigations
	  • Regulatory investigations
	  • Counselling on active client matters
	  • Non-public M&A activity (e.g. PwC acquisitions)
	• PwC insurance information (e.g., captive insurer's financial data, member firm insurance limits)
		All information
		• Sets of user credentials (user ID and Password or PIN number combinations) for a set of individuals. Credentials that control access to a PwC information or a hardware asset
		• Special categories of sensitive personal data:
		  • Race/ethnic origin /nationality/citizenship status
		  • Political opinions
		  • Religious or philosophical beliefs
		  • Trade Union status
		  • Genetic and biometric data
		  • Health information / medical records / Disability status
			• Non-public financial performance or otherwise price sensitive data
			  • draft/unpublished government tax forms,
			  • pre-issuance financial statements
			  • assessments and reports of internal financial controls
			  • valuations
			  • M&A work that is stock market price sensitive (where insider trading rules would apply)
			  • restructuring
			  • redundancies

		• Covered Information: Protected Health Information (PHI or ePHI), any information in a medical record that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment. • Criminal records or allegations of criminal offense • Sex life / sexual orientation • Government issued ID numbers (SSN, Passport, driver's license) • Credit card / bank account /credit check / financial information **Partner and staff information** • Disciplinary records (ethics complaints, investigations, independence violations, reprimands) • Staff absence records, sick or disability leaves (health data) **Client and others' information** • Large data sets of PII which have not been aggregated or anonymised (e.g. payroll file for a department or member	• Highly sensitive Intellectual Property (e.g. for cutting edge technology or high-profile designs and inventions) • Names of client board members that are not publicly available • Classified Information (e.g. information government entities identify as "classified")

		firm, client downloaded financial information) • Client stored, processed or transmitted cardholder data	

Data Management

PwC's data should be managed in a systematic and structured manner, and information security requirements must be maintained throughout the data lifecycle. Additional guidance for data handling, transfer, storage and archival considerations both electronic and physical must be given for sensitive data classified as confidential and highly confidential.

Application owners must implement logical or physical separation where an application or system stored or processes personal data for individuals residing in any European Economic Area (EEA) (e.g. Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK)

Reference to latest list: https://www.gov.uk/eu-eea

Additional Privacy Assessments: A data protection risk assessment is recommended where an application owner is unable to confirm segregation of personal data for an individual in EEA. Application owners or client engagement teams must complete a data protection impact assessment when the data protection risk assessment results are identified as high risk.

Data Handling (Includes Transfer)

All Information Users must follow the data handling and transfer guidelines from data creation to destruction. Be advised that detail engagement-specific security controls may be required when handling client data.

Applications, systems and client engagement teams that perform marketing efforts must support user consent selection and potential for change in consent to share personal data.

Applications that leverage user tracking mechanisms (e.g. cookies) must provide disclosure and support opt-out options from any given individual.

Data Storage (Includes Archive)

Data storage includes electronic and physical storage of media. Archive includes disposal and destruction of data at the end of its lifecycle.

Data must be retained in accordance with the original intended purpose and securely disposed of at the time of expiration. Applications, systems and client engagement teams must implement process or technical controls to support legal or data subject access request holds to adequately preserve data as needed to support legal requirements.

An application or system that stores or processes personal data must provide a notice of collection to the individual (data subject). Member firms must track data subject access requests in a centralized tool.

ISP Data Handling Rules specific to Data Classification

The chart below has three categories as defined;

Not Required	Implementation of a control is **not necessary** for the specific data classification identified.
Recommend	Implementation of a control must be implemented **whenever possible** for the specific data classification.
Required	Implementation of a control is **mandatory** for a given data classification.

	Public	Internal	Confi dential	Highly Confidential
Data in Use				
Access and Approvals				
Restrict access to a 'need to know' basis.	Not Required	Recommend	Required	Required
Information Owner or approved designee must be an additional approver for access to information systems containing data. (e.g. internal human capital, accounting)	Not Required	Recommend	Required	Required
Information Owner or approved designee must establish access rights / distribution requirements for data. (e.g. share drives, collaboration sites, direct data access)	Not Required	Recommend	Required	Required
Information Owner or approved designee must review access rights to data periodically or when classification levels change.	Not Required	Recommend	Required	Required
Information Owner or approved designee must approve removal of data from Firm premises.	Not Required	Recommend	Required	Required
Information Owner or approved designee must approve sharing of data internally.	Not Required	Not Required	Required	Required
Information Owner or approved designee must approve sharing of data externally.	Not Required	Required	Required	Required
Non-disclosure or confidentiality agreement must be in place with individuals or third-parties prior to sharing data.	Not Required	Required	Required	Required

	Public	Internal	Confidential	Highly Confidential
Background checks, where legally permissible and training for PwC employees and staff must be completed prior to granting access to data.	Not Required	Required	Required	Required
Marking / Labelling				
Removable storage media must include a label on the exterior of the container. Label must not be easily removable and include at a minimum: • Asset number as assigned by IT, details for return using a general support phone number and must not indicate the PwC company or brand on the label (e.g. NOT include PwC name, address, individual contact information) to prevent from highlighting a sensitive asset.	Required	Required	Required	Required
All electronic data (e.g. PwC reports, spreadsheets, PowerPoint and PDF documents) must be labelled in the metadata per classification level and include distribution limitations in the footer, where applicable. (e.g. Internal Use Only, Confidential Document)	Not Required	Recommend	Recommend	Required
Clearly mark classification on physical medium.	Recommend	Recommend	Recommend	Recommend

Photocopying				
Permission from the Information Owner should be obtained prior to making any copies or taking any photos (e.g., using phone, camera, or other device) of data. Highly confidential data to be distributed should have a unique identifier for each recipient the data is shared with.	Not Required	Not Required	Not Required	Recommend
Copies of the data follow the same storage and handling requirements as the originals.	Required	Required	Required	Required
Use of collaboration tools to share data must be controlled to include only authorised participants. (e.g. recommend using controls like web ex passcodes/passwords)	Not Required	Recommend	Recommend	Required
Printing, Scanning or Faxing				
Data must be printed, scanned or faxed from and to individuals using a secured ID or within a secured area.	Not Required	Not Required	Recommend	Required
Receipt confirmation of faxed or remotely scanned or remotely printed data sent externally to an individual must be acknowledged.	Not Required	Not Required	Recommend	Required
Printers, scanners, and fax machines must not retain the data upon completion of job.	Not Required	Not Required	Recommend	Required
Voice				
Be aware of surroundings when reading, discussing, or otherwise communicating data in public places (e.g., airplanes, restaurants, elevators, cell phone conversation, hangouts, etc.).	Not Required	Recommend	Required	Required
Refrain from leaving messages containing data on answering machines or voicemail systems. Best practice is voice mail retention of no more than 7 days.	Not Required	Recommend	Recommend	Required
Conference call discussions around data must include only authorized participants (e.g. recommend using	Not Required	Recommend	Required	Required

controls like web ex passcodes/passwords)				
Foreign Travel				
Refer to Member Firm local travel policies where applicable.				

Data in Motion/ In Transit				
E-mail Exchange				
E-mail attachments must be encrypted using approved methods (e.g., WinZip with 256-bit, PGP, or minimum 128-bit encryption, etc.). Highly confidential data must not be included in the body of an email message to prevent mistaken distribution.	Not Required	Not Required	Recommend	Required
Passwords for encrypted files must be provided through a separate channel other than email (e.g. phone, fax, SMS text message) and follow PwC minimum password complexity requirements defined in the Global ISP.	Not Required	Not Required	Recommend	Required
E-mail should only be sent to named individuals and not to group E-mail distribution lists or addresses.	Not Required	Not Required	Recommend	Required
Transport (General)				
Data sent outside of the PwC network should be transferred using a secure file exchange service or process (e.g. PKI enabled website, client hosted secure FTP, MFT-2Go)	Not Required	Recommend	Recommend	Required
Must only take hard copy documents from office if transferred directly between office/home/client. (not via pub, bar, gym, restaurant, etc.)	Not Required	Not Required	Recommend	Required
Pickup, receipt, transfer, and delivery of information media must be restricted to authorised personnel or approved courier. Automated tracking and accountability controls should be used.	Not Required	Recommend	Required	Required

Must obtain client approval to transport hard copy or electronic copy data from client site.	Not Required	Recommend	Recommend	Required
Delivery of hard copies be sealed in a package with a return address provided and sent only to designated authorized individuals who confirm receipt of delivery. (e.g., via phone call, individual mail, signature, etc.).	Not Required	Recommend	Required	Required
Refer to local member firm secure workspace and acceptable use policies for additional data handling requirements.				
Data Storage / at Rest				
Storage on Information Systems (File shares, databases, etc.)				
Data must only be stored in approved information systems and locations (e.g., SharePoint sites, LN databases, share drive folder, etc.).	Not Required	Required	Required	Required
Only authorized individuals may have access to data in information systems, related backups and access be reviewed periodically as appropriate.	Not Required	Recommend	Required	Required
Storage on Removable Media (USBs, CDs, Backup Tapes, etc.)				
Only approved removable media devices can be used to store data and data must be protected with an approved encryption method. (e.g. PwC encrypted USB drives (memory sticks) or WinZip encrypted files for CDs and DVDs.) *Additional client approval and restrictions may apply.	Not Required	Required	Required	Not Allowed *Exception Required
Password protected device, file or media must be used.	Not Required	Required	Required	Required
Must not use portable media as permanent storage as should be stored on system of records. Delete contents of memory sticks before and after use. Copy to PwC network any files created on smartphones or tablets.	Not Required	Required	Required	Required
Storage on Personal or Mobile Devices (Smart Phones, Tablets, Laptops, etc.)				
Device must be protected with password or PIN with forced timeout set to lock and secure device when not in use.	Not Required	Required	Required	Required

Device must be configured to allow remote wipe by Firm MDM solution.	Not Required	Required	Required	Required
Unattended devices must be powered down or in hibernate mode when outside the office or end of use.	Required	Required	Required	Required
Must use PwC IT approved systems and equipment	Required	Required	Required	Required
Retention, Disposal, and Destruction of Stored Data				
Unless subject to legal hold, electronic information required as a record (to evidence work undertaken on engagements or otherwise to support the operations of the firm) should be transferred to and stored on the appropriate system of record and deleted at the end of its specified retention period.	Not Required	Required	Required	Required
Unless subject to legal hold, duplicate or superseded versions of records and electronic information that is not a record should be deleted at the end of the engagement or, at a maximum, two years after its last modification.	Recommend	Recommend	Required	Required
Physical Security				
Individual workspaces should be clear of all data and media when not in use.	Not Required	Required	Required	Required
Hard copy materials should be stored in a controlled area and locked in a file container / drawer / cabinet when not in active use. Includes storage in locked safe in hotel left unattended.	Not Required	Recommend	Required	Required

Application Control Requirements

The table below provides additional guidance for information system requirements to implement security controls based on the levels of data classification.

	Public	Internal	Confidential	Highly Confidential
Application Requirements				
Authentication & Authorisation				
External system interface and end user to application	Not Required	Single-Factor	Multi-Factor	Multi-Factor
End user or client calling an application or service	Open Access	Controlled	Controlled	Controlled
Managing Authenticated User Sessions	Not Required	Timeout Inactive 4hr. session max 8hr.	Timeout Inactive 20 min. Session max 8hr.	Timeout Inactive 20 min. Session max 8hr.
Application Resource Permission	Least Privilege	Least Privilege	Least Privilege	Least Privilege
Data Security Training Required Prior to Access	Not Required	Not Required	Required	Required
Data Protection				
Data in transit	Unencrypted	Encrypt from end-user to app.	Encrypt All Communication	Encrypt All
Data at rest	Unencrypted	Unencrypted	-Encrypt external facing / hosted - New apps	Encrypt All
Application and data segregation	Not Required	Not Required	Dedicated for Restricted	Dedicated
Validating Input and Output Data	Required	Required	Required	Required
Audit Trail	Optional	Required	Required	Required
Production data allowed in Non-Production environments	Allowed	Allowed	Sanitised/ Masked	Sanitised/ Masked
Third Party and Hosting				
Application hosting external	Allowed	Allowed	Allowed	Allowed in Isolated Env. w/NIS approval
Oversight of Third Party Suppliers	Not Required	Not Required	Independent Verification	Independent Verification
Security Assessment				
Vulnerability, static code review and penetration testing prior to production implementation	Source Code Scan; Pen Test every 3 years	Source Code Scan; Pen Test every 3 years	Source Code Scan; Pen Test annual	Source Code Scan; Pen Test annual
Web Application Security Assessment	Required	Required	Required	Required
Mobility Computing				

	Public	Internal	Confidential	Highly Confidential
Mobile Applications	Not Required	Isolated	Isolated & Encrypted	Isolated & Encrypted

Appendix A - Common Terms and Definitions

Term	Definition
Information Owners	Information Owners are individuals, teams or functional managers who are responsible and accountable for the security and protection of their information and information assets. The Information Owner is dependent on whether the data is considered sensitive because of client determination or PwC determination (e.g., Public, Internal, Confidential, and Highly Confidential). For client data, the Information Owner is the Engagement Leader or the assigned Access Control Owner (ACO).
Information User	Information Users are individual Firm personnel who are responsible and accountable for abiding by the ISP, data classification framework and understanding the value of information and information assets. Users should be proactive in identifying, communicating (to the Information Owner), and correcting any misclassifications.
Personal Data	Any information about a person or from which a person can be identified. Personal data need not be tied to a name and can include public data. If a person cannot be identified or re-identified from the data, the data is not personal data. NDPP Definition: Any information that identifies or can potentially be used to identify, contact or locate an individual. This includes information that can be linked with identifiable information from other sources, or from which other personal information can easily be derived. (Some examples: Name, Personal email address, cell phone number, employee ID/GUID, job history and education, marital status, date of birth with year, salary and bonus, IP address)
PwC	"PwC" is the brand under which member firms of PricewaterhouseCoopers International Limited (PwCIL) operate and provide services.
Sensitive Data	Personal Data or Confidential Information that is sensitive due to its nature and should be handled in accordance with the Data Classification Standard.
System Owner	System Owners are individuals or teams responsible and accountable for the security and protection of Firm information systems.