Synchrony Financial

Information Security Policy

Issued By: Information Technology

Approved By: Synchrony Financial Risk Committee
Policy Owner: Information Security Officer
Policy Contact: Information Security Program Leader

Table of Contents

1 Applicability and Scope

1.1 Applicability

The Information Security Policy (hereafter referred to as the "**Policy**") applies to various operations within Synchrony Financial ("**SYF**"), its sales platforms, all employees and, as applicable, subsidiaries and affiliates that support SYF's business activities (collectively "**SYF Entities**").

This Policy establishes baseline requirements designed to protect the confidentiality, integrity, and availability of all SYF Financial data in electronic or physical form. In many instances, this policy requires heightened safeguards with respect to "SYF Restricted" or "SYF Confidential with Sensitive PII" data (each as defined in Appendix A and hereinafter "Covered Data"), reflecting SYF Financials' risk-based approach to mitigating information security risks.

1.2 Scope

This Information Security Policy (the "**Policy**") describes the SYF Information Security Program security control requirements. It applies to the Financial and to the various operations of the Financial and its business lines, and to all employees and, as applicable, affiliates and third parties that support the Financials' activities (collectively, "**SYF**"). This Policy establishes the minimum standards for all SYF Financial Entities.

2 Overview and Purpose

This Policy implements the SYF Information Security Program. SYF management ("**Management**") has developed and implemented a written Information Security Program ("**Program**") which is designed to:

- Reasonably ensure the security and confidentiality of sensitive business and customer information;
- Reasonably protect against any anticipated threats or hazards to the security or integrity of such information;
- Reasonably protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to SYF or any customer; and
- Reasonably ensure the proper disposal of customer digital information.
- Reasonably report the state of security to management and relevant committees

This Program is applicable to all SYF Entities. The SYF Information Security Officer ("**ISO**") has all appropriate authority to carry out all necessary activities in furtherance of the Program.

The Policy establishes baseline requirements designed to protect the confidentiality, integrity, and availability of all SYF Financial data in electronic or physical form. In many instances, this Policy requires heightened safeguards with respect to "SYF Restricted" or "SYF Confidential with Sensitive PII" data (each as defined in Appendix A and hereinafter "**Covered Data**"), reflecting SYF Financials' risk-based approach to mitigating information security risks.

3 Policy Content

3.1 Definitions

The following terms and acronyms are used within this document.

Term	Definition
CDI	Company Directory
CIO	Chief Information Officer
COE	Center of Excellence
Data Center	Refers to a facility or site that hosts SYF Entity servers and communications equipment (e.g. IVR, PBX).
Encryption	The act of converting data or information into code in order to prevent unauthorized access. Encryption is used to provide message confidentiality and enable secure transmission of sensitive data.
ERMC	Enterprise Risk Management Committee
Function	Refers to the major infrastructure support units as defined by SYF. These include: Compliance, Finance, Human Resources, Information Technology, Legal, Operations, and Risk Management.
Function Leader	Executive of the major infrastructure support unit as defined by SYF.
HPA	Highly Privileged Access Advanced access privileges that may include the following: System-level administrative access Administration of accounts and passwords Any additional accounts considered by the SYF business or system owner to pose a high risk (i.e. Database Administrators)
Incident	A violation of the confidentiality, integrity, and/or availability of a company information resource. Disclosure, degradation, loss, and denial of data or the computing platform are the typical consequences of an Incident.
Information Asset	A definable piece of information, stored in any manner which is recognized as “valuable” to the organization.
Information/Data Owner	An information or data owner is accountable for the accuracy and integrity of its business information or data within applications or business process.

Term	Definition
ISO	Information Security Officer
IT Asset	Any data, device, or other component of the information technology environment that supports bank-related activities including but not limited to hardware (for example; servers and switches) and software (for example; mission-critical applications and support systems.
IT System	Collection of applications, databases, and servers which achieve a business-defined process.
Jump Box	A computer gateway on a network segment with access to those critical hosts and ports the box needs access to. Users need to log into the jump box prior to connecting to other machines on the critical network or hosts for their work.
Non-Personal Account	Any account which does not fit the definition of a Personal Account (an account belonging to one person for their exclusive use). This includes service, System and Emergency accounts.
PRG	Policy Review Group
SDLC	Systems Development Life Cycle
SSO	Single Sign On The preferred authentication method for all SYF web-based applications as currently implemented by Siteminder.
SYF	SYF Financial
SYF Workers	Includes SYF employees, contractors, contingent workers, temporary workers and, as applicable, SYF Entity employees.
Third Party	When used as either a noun or an adjective, means any entity, including joint ventures and sole proprietorships, in which SYF does not have majority ownership or control that is not SYF or one of its subsidiaries.

3.2 Information Security Internal Organization

3.2.1 Information Security Coordination

Information security strategic activities will be completed by the Information Security Officer (ISO) including strategic development and implementation of the Program.

3.2.2 Allocation of Information Security Responsibilities

The ISO is responsible for implementing and maintaining the Program and for reporting security status and metrics to the SYF Chief Information Officer ("**CIO**").

3.3 Third Parties

Risks emerging from relationships with Third Parties must be identified and appropriate controls must be implemented before granting access to systems or Covered Data.

3.4 Asset Management

3.4.1 Responsibility for Assets

3.4.1.1 Inventory of Assets

SYF must maintain a current inventory of IT Assets which must be reviewed by SYF IT management for accuracy and completeness at least annually.

3.4.1.2 Acceptable Use of Information Assets

SYF Workers are accountable for all activity associated with their user IDs. SYF employees are also responsible for compliance with the requirements of the GECC Acceptable Use of Company Information Sources Policy.

3.4.2 Information Classification

3.4.2.1 Classification Categories

SYF information must be protected in accordance with the following SYF data classification categories (Note – for purposes of this policy, SYF has adopted the GECC data classification categories *mutatis mutandis*):

- Public
- SYF Internal
- SYF Confidential
  - SYF Confidential with Sensitive PII
- SYF Restricted

For detailed information see Appendix A.

3.5 Human Resources Security

3.5.1 Employment

Background checks are performed for all SYF employees prior to on-boarding. SYF employees must accept and acknowledge their information security responsibilities as part of the on-boarding process within 45 days of employment.

3.5.2 Information Security Awareness, Education, and Training

SYF must have and maintain an Information Security Awareness Program. SYF employees who have access to SYF information must receive annual information security training and certify that they understand their information security responsibilities. In addition, non- SYF employees (contractors, contingent workers and temporary workers not directly hired by SYF), who have access to SYF data, must be made aware of their information protection obligations, by their employers, through contract terms.

3.5.3 Termination or Change of Employment

3.5.3.1 Termination and Removal of Access Rights

Managers must submit an off-boarding request using their local off-boarding procedure by or before the next business day in the event of an employee termination.

Physical building access, SSO, Active Directory and remote access rights must be disabled for all terminated SYF Workers within 24 hours of termination in the Company Directory (CDI). Access to other systems that can access Covered Data must be disabled within 32 days of termination.

3.5.3.2 Change of Employment

Managers are responsible for submitting a transfer process request when an employee's role significantly changes, such as a new business segment, manager and location. When a manager initiates the transfer process, they should note if current access rights should be retained or revoked.

3.5.3.3 Return of Assets

Managers are responsible for ensuring that SYF Workers return SYF assets in their possession at the termination of their employment or contract in accordance with the SYF Acceptable Use of Company Information Sources policy and local laws and regulations.

3.6 Physical Security

3.6.1 Working in Secure Areas

SYF and SYF Entity Data Centers and Third Party hosting facilities must have physical security controls in place that prevent unauthorized individuals from gaining physical access. These controls include:

- Physical access to Data Center rooms must be secured at a minimum to include locked doors, cameras and badge readers.
- Access to Data Center facilities must be limited by job function
- Access to Data Center facilities must be approved and logged
- Access logs to Data Center facilities must be reviewed on a semi-annual basis to ensure that only appropriate access is granted

- SYF and SYF Entity equipment in Third Party facilities shared with non- SYF Customers must be physically segregated from non-SYF equipment by using either locked cages or racks
- ID badges must be issued to individuals before access is granted to facilities

3.6.2 Secure Disposal or Re-use of Equipment

SYF data as well as licensed software must be removed from computer equipment and removable media prior to disposal or re-use. Secure methods of disposal such as wiping, degaussing or physical destruction are acceptable. No disposal or destruction shall take place without confirming that the data has reached the end of its applicable retention period and that there is no additional retention period (such as a litigation hold or preservation notice).

Other technology, including photocopiers, fax machines and printers may contain a hard drive or flash memory that stores SYF data in various forms, such as digital images of documents sent to the device. SYF must have a process in place that ensures that SYF data is erased, encrypted or rendered unreadable prior to the device being returned to the leasing company, sold or otherwise decommissioned.

3.7 Communications and Operations Management

3.7.1 Segregation of Duties

User account creation requests and access entitlement requests must not be self-approved by the requestor. Managers or their delegates cannot review or approve their own access entitlements.

3.7.2 Protection Against Malicious Code

SYF-provided anti-malware software must be installed, automatically updated and functioning on all SYF-provided Microsoft Windows desktops, laptops and servers where technically feasible.

3.7.3 Network Security Controls

- Only SYF -approved Wireless Local Area Networks (WLANs) may be connected to the SYF network.
- All external networking connections must be made through SYF-managed network infrastructure and must include network security monitoring.
- Where inbound access modems are in use, controls must be in place commensurate with system risk to ensure that access is for authorized purposes only.

3.7.4 Management of Removable Media

Covered hard drives that are stored on removable media such as compact disk CD, DVD, diskette, USB devices, portable hard drives, magnetic tape, or optical disk must be encrypted using SYF-approved encryption technologies.

3.7.5 Exchange of Information

3.7.5.1 Physical Media in Transit

Covered Data that is shipped on removable media (including tape, CD, DVD, USB) must be encrypted using SYF-approved encryption technologies or secured using a secure courier service.

3.7.5.2 Electronic Messaging

Covered Data that is transmitted outside the SYF network (using methods including but not limited to email, file transmissions, instant messaging and HTTP) must be encrypted using SYF-approved encryption technologies, in accordance with local laws and regulations.

3.7.6 Monitoring

3.7.6.1 Audit Logging

This section is applicable for Operating System (OS) logging at a minimum.

Security-relevant events must be logged and reviewed on a periodic basis (no less frequent than quarterly), commensurate with the risk and criticality level of the information resource. Logs must be retained in compliance with SYF data retention requirements.

The following security-relevant events are considered minimum auditing requirements:

- Account creation
- Security privilege allocations or changes
- Password resets
- Successful and unsuccessful system login
- Security configuration changes
- User-ID, Date/Time, Terminal ID and IP address

In addition, Highly Privileged Access (HPA) must be logged, reviewed and protected from unauthorized use of the account where technically feasible. Exceptions must be documented and approved by the SYF ISO. HPA audit logs must include all of the above requirements as well as:

- The application or process being accessed
- Any read or update access to Covered Data
- Changes to, or attempts to change, system security settings and controls

The frequency of review is dictated by the volume of data and should be no less frequent than weekly. In many locations, the data volume may require daily review.

All monitoring activities must be in compliance with local legal requirements.

3.7.6.2 Protection of Log Information

System administrators are responsible for the protection and integrity of audit logs and must ensure that log files cannot be deleted or modified. Audit logs must be kept in compliance with local and business data retention requirements.

3.8 Access Control

3.8.1 System Access Control

Access controls are required for all SYF IT systems commensurate with risk. Managers are accountable for the access rights of the users under their supervision. All access controls must support:

- Granting least privilege required for a particular role or function
- A denied list of access approvers

In addition to the above, SYF systems containing Covered Data must support:

- Restrictions and enhanced monitoring for HPA accounts (see section 7.6.1 Audit Logging and 8.2.2 Restricting HPA)
- Periodic review and removal of access rights (see section 8.2.4 Review of user access rights).

3.8.2 User Access Management

3.8.2.1 User Registration and Account Management

- There must be a formal procedure in place for granting and revoking access to all SYF IT systems.
- User IDs must be unique and traceable to a SYF employee who is responsible for this account
- Non-personal accounts must be traceable to a SYF employee that is responsible for the account. Default software and hardware accounts must be restricted by either disabling them or by maintaining an audit trail traceable to a unique individual. Use of default accounts must be monitored.

3.8.2.2 Restricting HPA

Security controls must ensure that HPA is only provided to individuals whose identity is established and their activities must be limited to the minimum required for business purposes.

- A user ID with HPA rights must be assigned only to an individual or if it is a service account with interactive log in rights, it must have a single designated responsible owner to manage account access and maintain accountability
- HPA job roles and responsibilities must be clearly defined
- Access must be limited to minimum privilege to meet the job requirements of the role
- HPA approvals must be performed by SYF employees as part of the provisioning process

- HPA process must undergo periodic SYF management review, at least quarterly
- Where technically feasible HPA must be provisioned on an as-needed basis and revoked when it is no longer needed
- HPA access must not occur using handheld or PDA devices

3.8.2.3 User and Non-Personal Password Management

The allocation of user passwords must be controlled through a formal process. This process must include the management of temporary and default passwords, recovery, reuse, expiration, complexity, length, lockout, storage and transmission requirements.

3.8.2.4 Review of User Access Rights

Accounts that access Covered Data must be reviewed quarterly, using a documented process. The review process must ensure that SYF Workers who have left SYF no longer have active accounts and that unnecessary entitlements have been removed when roles have changed.

3.8.3 User Responsibilities

3.8.3.1 Password Use

Passwords must not be written down or stored in clear text. In addition:

- Users must ensure that the passwords are kept confidential and must not be shared or disclosed to anyone including the IT Help Desk
- If a temporary password has been provided to the user, it must be changed immediately upon the next logon

3.8.3.2 Secure Workspace

All SYF Workers are required to protect SYF information in digital and in physical format that is used or stored at their workspace. Covered Data must not be left in open view after general business hours and must be kept in locked cabinets or drawers.

Covered Data in printed format must be disposed of in a secured shredding bin or a paper shredder in accordance with retention periods in the relevant Records Retention schedule.

3.8.4 Network Access Control

3.8.4.1 Personal Computer Hardware Use

Computing and network resources provided by SYF are intended for use only by authorized SYF Workers and Third Parties.

Personal computer hardware encompasses any hardware not provided by SYF or a SYF Entity, including hardware provided by consultants, such as PDAs, personal home computers and network equipment. Personal computer hardware can only be connected to the SYF network using an approved SYF process. SYF Workers should consult SYF ISO to determine if personal computer hardware is allowed.

3.8.4.2 Segregation in Networks

SYF networks must provide segregation between internal and external networks. External networks, such as de-militarized zones (DMZs) or Third-Party networks must be segregated from the internal network through the use of firewalls or other SYF-approved perimeter controls.

3.8.5 Mobile Computing and Communications

Encryption is mandatory for all SYF managed laptops subject to local laws and legal restrictions.

SYF managed PDAs and Smartphones must have password protection enabled on the device or the encrypted container containing SYF data. Employees are required to notify their manager or the IT Support desk within 24 hours after the employee is aware that a device was lost so that the remote wiping procedure can be initiated.

3.8.6 Telecommuting

Remote access to the SYF network is only permitted where there is a legitimate business need and management approval. Remote access must use SYF technology-approved solutions that employ two-factor authentication.

3.9 Information Systems Acquisition, Development, and Maintenance

3.9.1 Application Security Assessment

Information Security requirements must be included in the application Software Development Life Cycle ("**SDLC**") process.

Any new or planned Internet application must have an application security assessment performed prior to going live. All internet-facing applications are required to have a security assessment at least every 24 months. Internet facing applications are subject to a risk assessment to determine the need for enhanced authentication controls including multifactor authentication. Internal applications containing Covered Data must have a security assessment every 24 months. Security testing is to be performed by a SYF approved security testing facility only, including the SYF Corporate Application Security Center of Excellence (COE). Please consult the SYF ISO for acceptable alternatives.

Remediation for critical and high risk findings on all in-scope applications must be completed within 90 days of issue identification and verification.

3.9.2 Cryptographic Controls

3.9.2.1 Use of Cryptographic Controls

Use of encryption must follow applicable local laws and regulations. Where employed, cryptographic controls must follow the requirements outlined in SYF standards.

3.9.2.2 Key Management

Production cryptographic key management functions must ensure that encryption keys are securely managed during their entire lifecycle, including their generation, storage, use, revocation, recovery and destruction.

3.9.3 Protection of Data in Non-production Environments

Covered Data must be protected in both production and non-production environments, including maintaining an audit trail. Non-production environments using this data must either:

- Scrub, scramble or sanitize sensitive data or sensitive data fields to reduce the classification level; or
- Where the above is not possible, implement controls commensurate with the production environment

3.9.4 Securing Endpoint Computing for Highly Privileged Access Users

Any computer used for Highly Privileged Access (HPA) must have the at least the following data loss controls in place:

- Disable removable storage (ex. USB/CD/DVD)
- Block or monitor file transfers of Covered Data
- Block or monitor HTTP (Web) file uploads of Covered Data
- Restrict ability to email Covered Data

3.9.5 Management of System and Network Vulnerabilities

Minimally, quarterly security assessments must be conducted across SYF systems and networks to detect information security vulnerabilities.

Vulnerabilities and system patches must be prioritized for remediation commensurate with the risk to SYF systems, networks and data.

3.9.6 Information Security Incident Management

The Information Security Incident Management process provides a consistent process for identifying, reporting, investigating and closing information security incidents.

3.9.7 Reporting Information Security Incidents

SYF Workers must immediately report information security Incidents, subject to local law and any legal restrictions on such reporting.

Any questions on whether an event is considered an information security Incident should be directed to the SYF ISO, Chief Compliance Officer or Privacy Officer.

Spam email messages are not considered security Incidents and should d be reported following SYF reporting process.

3.9.8 Management of Information Security Incidents

SYF must have an established incident response process. This process must include roles, responsibilities, reporting, coordination, and communication.

3.10 Business Continuity/Disaster Recovery Security Management

When initiated and active, business continuity/disaster recovery environments must have the same information security controls found in the production environment.

3.11 Compliance with Security Policies and Standards

SYF information security practices and processes must be reviewed for compliance with the SYF Information Security Policy requirements on an annual basis. This process will be managed by the SYF ISO and will help to assess the adequacy of security controls based on changes to processes, technology and sensitivity of information. Issues that are identified as a result of this process must include a remediation plan.

3.12 Roles and Responsibilities

SYF CIO: The SYF CIO serves as the sponsor of the Program.

SYF ISO: The SYF ISO develops and implements the Program across SYF. Interpretive issues should be addressed with the ISO.

4 Policy Maintenance

4.1 Authority and Delegation

The Enterprise Risk Management Committee ("**ERMC**") and Risk Committee have approved this Policy. The Risk Committee hereby delegates to the ISO responsibility for the Policy and its maintenance, including authority to review and approve procedures established in accordance with the terms of the Policy. The SYF CISO is responsible for all interpretative issues relating to this Policy.

Any authority that the Risk Committee grants and any responsibility that the Risk Committee assigns to an officer under this Policy may be delegated by such officer in his or her discretion except as otherwise provided in this Policy.

4.2 Policy Review, Renewal and Approval

Except as delegated to the Policy Review Group ("**PRG**"), the ERMC and Risk Committee will review and approve this Policy periodically, but no less frequently than annually, and will be responsible for approving all material changes to the Policy and its appendices. The evidence of review and approval of this Policy shall be the meetings minutes in which such review and approval occurred. The ISO will review and approve related procedures (if any) periodically, but no less frequently than every three (3) years.

Periodic Review: The SYF Information Security Officer shall review this Policy on an annual basis to evaluate its effectiveness and accuracy. Any resulting material revisions shall be submitted for approval to the PRG, ERMC and Risk Committee and documented in the Revision History. If no material revisions are needed, the SYF Information Security Officer shall communicate the outcome of the review to the PRG.

Periodic Renewal: The PRG, ERMC and Risk Committee shall renew this Policy on an annual basis.

Approval: Initial approval of this Policy, as well as approval of any material changes, shall be by the PRG, ERMC and Risk Committee. The ERMC delegates to the PRG the authority to approve any non-material changes. Approvals shall be documented in Section 8.0 Revision History and in the Policy & Procedure Matrix.

Additional Triggers: Certain events, including but not limited to audit findings or changes in business activities, shall trigger unscheduled additional review and revision to this Policy.

5 Exclusions, Exceptions, and Violations

5.1 Exclusions and Special Situations

The Policy Owner will be responsible for identifying any areas of potential non-compliance. Following a determination of non-compliance, the non-complying sales platforms, function, or individual must establish an action plan to remediate their processes to comply with this Policy. Action plans must include a timeline and identified responsible party to oversee implementation of the action plan. The action plan must be implemented within an amount of time that is agreed upon and documented by the Policy Owner.

If local laws or regulations establish a higher standard than what is provided by this document, SYF must comply with those laws. If local requirements require a less stringent standard than that established by this Policy, it must be brought to the attention of the SYF ISO who, in consultation with counsel when appropriate, shall determine which standard should prevail.

Information security risk assessments and measurement processes shall be adopted in the development of the Program. The ISO will be responsible for identifying any areas of potential non-compliance under this Policy through annual self-assessments.

As used herein, an “exception” is a state of non-compliance with, or gap against, the requirements of this Policy which non-compliance or gap must be remedied as set forth below. An “exemption” is a state of non-compliance or gap for which formal permission has been granted and it is not subject to either this Policy, or to one or more sections within this Policy with regard to such non-compliance or gap.

In the event of non-compliance with this policy:

- A request for a temporary exception must be made to the SYF ISO and an action plan must be established to close the gap. These plans must be documented with a

clear timeline for closure and an identified responsible party to oversee implementation of the action plan; or

- The SYF ISO may grant an exemption from the requirements of this Policy that the function does not comply with, with the rationale and compensating controls clearly documented and maintained and reviewed annually.

The SYF ISO will have the primary responsibility of granting both exceptions and exemptions.

5.2 Violations

Violations of this Policy result in internal control weaknesses and / or failure to comply with applicable laws and regulations. Violations may result in employee disciplinary action, including termination in accordance with SYF policies and applicable law. Violations will be reported immediately to the SYF Chief Compliance Officer and General Counsel.

6 Contacts and Escalation

6.1 Contacts

- SYF Information Security Officer
- SYF Information Security Program Leader

6.2 Escalation

In the event there are conflicts in interpretation or implementation efforts pursuant to the terms of this Policy, the conflict should first be brought to the attention of the SYF Information Security Officer. If they are unable to address the conflict, it should be escalated to the PRG and beyond.

7 Cross References

7.1 Related Standards and Procedures

- SYF IT-S033 Encryption Standard
- SYF IT- S014 Key Management Standard
- SYF IT-S003 Password Standard
- SYF IT-S007 Third Party Information Security Standard

7.2 Related Policies

- GECC Acceptable Use of Company Information Sources Policy
- SYF Business Continuity Management Policy

7.3 Related Critical-to-Compliance Entries

- CTC – 349

- CTC – 478
- CTC – 479
- CTC - 715

7.4 Related Committee / Sub-Committee Charters

- IT Steering Sub-Committee Charter

8 Appendices

8.1 Revision History

The chart below contains a history of revisions to this document.

Version	Approval Date	Effective Date	Changes: Material / Non-Material	Description of Changes:
1	09/18/2014	09/18/2014	Initial version	Initial version

8.2 Appendix A: SYF Data Classification

SYF is responsible for classifying and protecting data according to the SYF Data Classification Standards and this Policy using the following four data classification categories:

Public

Public information is non-sensitive information available for public disclosure. Examples of Public information include press releases, company advertising (once approved for issuance), or other information where there would be no harm to SYF as a result of its availability to the general public.

SYF Internal

For purposes of this Policy, SYF Internal information means information belonging to SYF and not for disclosure to the public or external parties. The information is generally available to employees and authorized Third Parties and its release to the general public would cause limited harm to SYF. Examples of SYF Internal information include company organization charts or telephone directories.

SYF Confidential

For purposes of this Policy, SYF Confidential information means information that is sensitive or confidential within the company and intended for business use only by those with a need to know. Examples of SYF Confidential information include, but are not limited to, communications protected by attorney-client privilege, customer or supplier contracts, or personally identifiable customer or SYF personnel information (e.g., EMS data, compensation data, credit reports or creditworthiness assessments). Unauthorized disclosure of such information could cause significant harm (e.g., legal or financial liability; harm to SYF's reputation).

This Policy also recognizes the following concept as a subset of SYF Confidential:

SYF Confidential with Sensitive PII

For purposes of this Policy, SYF Confidential with Sensitive PII refers to any sensitive personally identifiable information that is not publicly available regarding any SYF employee, customer, or commercial customer (i.e., legal or natural person) of SYF. As reflected in the table below, SYF Confidential with Sensitive PII refers to "toxic combinations"—recognizing that certain data elements, when on their own, do not present risk to SYF or its customers unless combined with information that can tie it to a particular individual or entity. SYF Confidential with Sensitive PII includes, but is not limited to identifiers such as a name, address, user ID or telephone number in conjunction with a bank account number, credit or debit card processing elements (number, expiration date, or CAV), date of birth, driver's license number/other government ID number, mother's maiden name, personal identification number (PIN), Social Security Number (SSN), Tax Identification Number (TIN), a password, assessment of or report on the creditworthiness of the customer or other personal information such as racial or ethnic origin, health information, union membership, political views, or sexual orientation.

Note that the following table's "Sensitive Personal Information" column may not capture all data elements that are deemed sensitive by a particular jurisdiction. The ISO will work with counsel

to identify additional Sensitive Personal Information data elements, if any, within applicable jurisdictions.

Sensitive PII Examples ("Toxic Combinations")		
Personal identifier such as Name, Address, User ID, or Telephone Number	*In conjunction with any of:*	Bank account number (account providing direct access to funds)
		Credit/debit card processing elements (number, expiration date, or security code)
		Creditworthiness assessment or credit report
		Date of birth
		Drivers' license number/Other Government ID Number (e.g., passport)
		Mother's maiden name
		PIN (personal identification number)
		Social Security Number (U.S.) or other similar identifier
		TIN (tax identification number)
		Password
		Other Personal Information: • Ethnicity/race • Health information • Union membership • Political views • Sexual orientation

SYF Restricted

For purposes of this Policy, SYF Restricted information means information that is extremely sensitive or private, of the highest value to the company, which is intended for use by named individuals only. Examples of SYF Restricted information may include merger or acquisition related information, major trade secrets, strategic plans, or financial results prior to their release.

Encryption Requirements

Data Classification Type	Encryption Requirement
Public	None
SYF Internal	None
SYF Confidential	Encrypt on removable media
SYF Confidential with	Encrypt on removable media and when sent outside the SYF network in accordance with

Data Classification Type	Encryption Requirement
Sensitive PII	local laws and regulations
SYF Restricted	Encrypt on removable media and when sent outside the SYF network in accordance with local laws and regulations