



U.S. Bancorp Information Protection Posture

January 2019

Contents

Introduction	4
Information Protection Program and Principles	4
Risk Management	6
Security Policy	7
Third Party	7
Asset Management	8
Human Resource Security	9
Security Awareness and Training	9
Physical and Environmental	10
Communications and Operations Management	11
Access Control	12
Information Systems Application Development and Maintenance	13
Incident Event & Communications Management	14
Business Continuity and Disaster Recovery	15
Compliance	15
Mobile	16
Privacy	16
Software Security	17

Management's Assertion Regarding the Effectiveness of U.S. Bancorp Information Protection Program

As the management of U.S. Bancorp's Information Protection Program, we are responsible for designing, implementing, and maintaining an effective information protection program. As the Chief Information Security Officer (CISO), I have overall management authority and operational responsibility for the U.S. Bancorp Information Protection Program and for the full design, implementation, sustainability, and resiliency of the information security policies, processes, and controls. These policies and processes support the Business Lines in achieving security, confidentiality, integrity, and availability while meeting regulatory and compliance requirements.

U.S. Bancorp Information Protection Management asserts its Information Protection Program has sustainable processes that align with the Cybersecurity NIST framework that attest to the effectiveness of security, availability, and confidentiality policies, processes and controls with reasonable assurance, but not absolute, that controls are implemented to detect, remediate and prevent security events and safeguard customers information in compliance with policies.

Additionally, an independent assessment and opinion can be found in the U.S. Bancorp SOC reports. U.S. Bancorp SOC 2 reports are available upon request from a client that has signed a Non-disclosure agreement with U.S. Bancorp. SOC 3 reports are available upon requests from a client that does not have a signed Non-disclosure agreement.

Sincerely,

A handwritten signature in black ink, appearing to read "Tim J. Held", written over the printed name.

Timothy J. Held
Chief Information Security Officer
U.S. Bancorp

Introduction

U.S. Bancorp (the “Company”, which term shall include all subsidiary and/or affiliated entities, including, without limitation, U.S. Bank National Association, U.S. Bancorp Fund Services, LLC, Elavon, Inc. and Elavon Financial Services Ltd.) has a legal and ethical responsibility to ensure that its information is secure and private, is current and maintained accurately, and is available to authorized recipients when needed. U.S. Bancorp is also expected to obtain and process information fairly, keep it only for specified and lawful purposes, process data only in ways compatible with the purposes for which it was provided and ensure that only appropriate data is retained. Moreover, data is not retained longer than necessary to ensure compliance with legal, regulatory, contractual, and operational requirements.

To do this, the Company’s Information Protection Program is founded on a set of principles described within this document. The Company recognizes that some principles and associated controls may not be applicable to, or appropriate for every business environment.

The Company is committed to protecting the confidentiality, integrity, availability and privacy of customer data. Our reputation rests, in part, upon securely maintaining our customers’ information assets. The Company understands the importance of safeguarding all the information entrusted to us, regardless of who owns that information. All partner data is classified as “U.S. Bancorp Confidential” or “U.S. Bancorp Personal,” as are our trade secrets and customers’ personal information.

The Company also understands the importance of demonstrating our commitment to protecting customer information. This document provides a high-level overview of the Company’s information protection posture, which describes the commitment and resources we apply to information protection.

Information Protection Program and Principles

The Company maintains an Information Protection Program which relies on the following security principles:

- **Information and Information Systems are Assets:** The Company’s information assets are protected from disclosure, modification, deletion or loss in accordance with the sensitivity of the information and the risks associated with its disclosure to unauthorized individuals.
- **Information Security Risk Management:** The Company’s Information Protection Program aligns with *de facto* standards to manage well-known and well-understood risk(s). The program maintains processes to assess and manage risks to the security of the Company’s information as new threats emerge and as technology and business practices change. Compliance with information security policy is critical to managing information security risk.
- **Legal, Regulatory, and Contractual Compliance:** The Company’s Information Protection Program supports compliance with applicable laws, regulations and contractual requirements. The Company has mapped its information security policies to applicable legal, regulatory and contractual requirements including Gramm-Leach-Bliley Act (“GLBA”), Payment Card Industry (“PCI”), Health Insurance Portability and Accountability Act (“HIPAA”), Sarbanes-Oxley Act (“SOX”) and the National Institute of Standards and Technology (“NIST”) Cybersecurity Framework.

- **Layered Security (Defense in Depth):** The Company's Information Protection Program includes technical components at all levels of the infrastructure to significantly reduce the likelihood a weakness in one area does not lead to a compromise. Procedural controls are put in place wherever responsibility for security activities are assigned. Managerial controls ensure responsibilities are carried out and technical and procedural controls are functioning as designed.
- **Preference for Preventive over Compensating Controls:** Wherever feasible, reasonable controls are implemented to prevent security problems. Compensating controls are used as a second layer of verification for primary preventive controls, as appropriate, and as a substitute for preventive controls only where preventive controls are not feasible or not yet in place.
- **Restricted Access to the Enterprise Network:** Access to information assets is restricted to authorized individuals by minimizing the number of ways individuals may gain network access. A limited number of control points are maintained and exclusive use is enforced. Employee access to internal resources within the network is enabled by secure methods to access the Company's applications via the Internet, internal network access and administrative access to resources within the network.
- **Isolation of Critical and Sensitive Resources within the Enterprise Network:** Assets are classified according to their business criticality and sensitivity, and security resources are allocated to provide the greatest protection for the most critical and most sensitive (U.S. Bancorp Confidential and U.S. Bancorp Personal) assets. Network design and access controls support this protection priority.
- **Restricted Access Based on Level of Trust:** Access to information assets is controlled based on the level of trust of the individual seeking access and the security of the access path. Internal employees using U.S. Bancorp-supported computers within the network are more trusted than business partners connecting via the Internet; business partners are more trusted than prospective customers; etc. In general, the level of trust diminishes as the level of U.S. Bancorp control over the access of the individual or systems seeking access and the access path is reduced and as U.S. Bancorp's ability to verify the level of security of the accessing party or system and the access path decline. Access to assets within the network is reduced as the level of trust diminishes.
- **Business Control of Business Information Resources:** Technology and Operations Services ("TOS") maintains custody of information assets. Business line management controls the security of information assets they own. The Information Protection Program establishes and maintains processes for information ownership and access authorization to ensure adequate segregation of function through business line control for information assets.
- **Least Privilege and Access based on Business Need:** To ensure information confidentiality, availability and integrity, access to information resources is provided on a need-to-know and need-to-use basis, according to job roles and functions defined by the information owner. Where privileged access is required for those in custodial roles (generally, TOS) or business line IT staff responsible for the processing, storage, transmission, backup and secure handling of information), such access is limited, to the extent possible, to the level needed, within the specific role of each employee. Such individuals are educated on the risks and responsibilities related to having this access and agree to comply with restrictions on their

use of privileged authority.

- **Secure Application Design and Development:** U.S. Bancorp's Information Protection Program includes steps throughout the application life cycle (design, development, deployment, maintenance and retirement) to ensure the protection of information assets accessible through business applications.
- **Protection of Information Assets in the Custody of Third Parties:** When U.S. Bancorp information assets are placed in the custody of third parties, U.S. Bancorp retains responsibility for its protection to meet business, legal, regulatory and contractual requirements. U.S. Bancorp vests that responsibility with third-party relationship owners, who ensure contractual agreements provide for the protection of such assets (consistent with enterprise security policy) and guarantees U.S. Bancorp the right to verify the protection of its assets through its own audit processes or receipt of reliable third-party assessments.
- **Support of and Consistency with Other U.S. Bancorp Information Protection Practices:** U.S. Bancorp's Information Protection Program is a critical component of U.S. Bancorp's overall information protection program. It supports U.S. Bancorp's overall information protection objectives and is coordinated with other related programs, such as enterprise privacy, compliance, and risk management programs, to ensure clarity of purpose and a consistent message to all U.S. Bancorp employees and contractors responsible for protecting customer and U.S. Bancorp information assets.

In addition to the security principles, U.S. Bancorp Information Protection Program aligns with published NIST guidelines and other industry-accepted security standards. Employees and contractors apply these principles when protecting information, where applicable.

Risk Management

U.S. Bancorp's Information Protection Program is designed to identify, quantify (where possible), prioritize and mitigate risks to acceptable levels with the objective of maintaining the security management of enterprise information assets and intellectual property. In addition, the program utilizes a risk model to establish appropriate levels of priorities and actions needed for managing risks classified as Very High, High, Moderate, and Low.

U.S. Bancorp's Information Protection Program aligns with de facto standards to manage well-known and well-understood risks. The program maintains processes and methodologies to assess and manage risks to the integrity, confidentiality and availability of enterprise information assets as new threats emerge and as technology and business practices change. The program is governed by information security policies established by approval from the Information Security Steering Committee ("ISSC"). Compliance with information security policies is required in the absence of an approved risk record.

U.S. Bancorp's Information Protection Program implements layered technical and operational controls at all levels of the technology and business ecosystem to significantly reduce the likelihood a weakness in one area will lead to a pervasive compromise of information assets and intellectual property in other areas.

While the enterprise Information Protection Program requirements and controls are founded upon the principles identified within this document, appropriate requirements and controls for treating information security related risks to enterprise information assets and resources are determined based upon risk assessment activities. The recognition that some associated controls may not

be applicable or appropriate for every environment (business lines, departments, and information systems) is a guiding principle for taking a balanced approach to managing risks across distributed environments.

Security Policy

Information security policies are established and maintained to ensure compliance with legal, regulatory and contractual obligations. These policies are designed to protect confidential business and personal information. These policies are implemented through effective communication, training and enforcement. Information security policies form the basis of the Information Protection Program (Program). The Program also includes development and maintenance of security configuration baselines for all critical technologies used to store, transmit or process confidential information.

Information security policies are accessible to all employees on the internal corporate web portal. U.S. Bancorp holds all personnel accountable for understanding and complying with those policies. All information security policies are reviewed by the appropriate subject matter experts from Information Protection Services (“IPS”) and each of U.S. Bancorp’s business lines. Policies are then approved by the ISSC. Security policies establish written requirements for U.S. Bancorp Data Loss Prevention practices and other control processes to protect confidential and personal information through the stages of the information lifecycle.

Organizational Security

U.S. Bancorp’s Chief Information Security Officer (“CISO”) has oversight of the IPS organization and security operations within U.S. Bancorp, and reports directly to the Vice Chairman for TOS. The CISO has overall management authority and operational responsibility for the U.S. Bancorp Information Protection Program. The CISO presents and recommends significant modifications of the Program for approval by the Board or the ISSC. Additionally, the CISO reports on the overall status of the Program and U.S. Bancorp’s compliance with applicable laws, regulations and contractual obligations. The ISSC provides governance and oversight of IPS’ development and implementation of the U.S. Bancorp Information Protection Program.

The Information Protection Program undergoes regular audits performed by the internal auditors, Corporate Audit Services. U.S. Bancorp’s Information Protection Program is regularly reviewed by independent auditors and assessors, both internal and external, and federal regulators.

Functional areas within IPS are reviewed by auditors to ensure independent and objective assessments of the adequacy, effectiveness, and efficiency of risk extension, transfer and mitigation processes. The IPS department is comprised of Information Security Professionals organized by functional security teams reporting up to the CISO. Activities are aligned with the overall information protection strategy.

A formal report and information protection strategy are presented to the U.S. Bancorp Board of Directors. Updates are also provided to the Board regarding progress toward strategic goals and other updates. Metrics are communicated to senior management reflecting key performance indicators of the Information Protection Program.

Third Party

With respect to confidentiality agreements and third parties, non-disclosure agreements (“NDAs”) are executed by U.S. Bancorp any time U.S. Bancorp is engaged in dialogue or the exchange of information deemed sensitive or confidential to U.S. Bancorp. The only type of information exchange where an NDA would not be needed would be where information is generally known

or available to the public. The NDA/Confidentiality Agreement ensures sensitive or confidential information remains protected, and U.S. Bancorp has legal recourse in the event there is disclosure. NDAs are part of the checklist of artifacts considered during engagements with contractors, third party/hosted data center providers and others.

When a U.S. Bancorp line of business decides to enter into a business arrangement with another entity, it first determines whether U.S. Bancorp Personal information will be shared. If so, a security risk assessment is performed on the third party before a contract with the third party is executed. Security risk assessments help IPS determine both the information and physical security posture of third parties. These assessments are extensive and cover the prospective third party's policies, network architecture, computing environment, access control standards, intrusion detection, disaster recovery planning and auditing. As part of the engagement process, third parties must disclose high-level information on security risks and audit findings, correction of any problems discovered, and results of prior assessments.

Asset Management

Technology Assets

U.S. Bancorp has a formal, documented asset management program which tracks the treatment, handling, disposal, destruction and reuse of all assets that contain or possess customer information. The program is approved by management, communicated to the appropriate constituents and maintains appropriate asset management policies. In order to achieve and maintain appropriate protection of organizational assets, all valuable enterprise assets are accounted for, have a designated owner and rules for acceptable use. Owners are assigned responsibility for the maintenance of appropriate controls of assets. The implementation of specific controls may be delegated by the owner as appropriate, but the owner remains responsible for the proper protection of the assets. Each owner is responsible for maintaining an inventory of all critical assets (e.g., hardware, software, licenses) necessary for business continuity protections.

Assets are classified according to their business criticality and sensitivity, and security resources are allocated to provide greatest protection for the most critical and most sensitive (U.S. Bancorp Confidential and U.S. Bancorp Personal) assets. Network design and access controls support this protection priority.

Information Assets

Enterprise information assets are protected from disclosure, modification, deletion or loss in accordance with the sensitivity of the information and the risks associated with its disclosure to unauthorized individuals. U.S. Bancorp has established handling procedures and access controls commensurate with the data for each information classification. Handling practices related to storage provide reasonable protection of information, regardless of form, against unauthorized disclosure.

U.S. Bancorp's Information Security policies, along with the Clean Work Area Guidance ("Guidance"), provide the framework for personnel to protect information while handling it at their desks and in their work areas. The Guidance describes what personnel must do to maintain a clean work area while handling confidential information and helps personnel understand how to handle non-public information based on the classification, location, and volume of information.

Protection may include hardware, software or other mechanisms to appropriately control access to U.S. Bancorp Confidential or U.S. Bancorp Personal information. Information classified as Personal is not to be used or requested in business processes that do not strictly require it. U.S.

Bancorp personnel are not allowed to divulge, use or attempt to access customer information except in a manner consistent with stated services to the customer and for authorized business purposes. Non-Disclosure Agreements must reflect this intent. Personal information must not be copied from secure locations. This includes dedicated application databases or other locations where access is limited by role and is transferred to locations not managed with the same access controls. However, if the storage is temporary to support a business need, the file is removed or deleted immediately after the business need is fulfilled.

Human Resource Security

Security responsibilities are addressed in job descriptions, terms and conditions of employment and required training to ensure employees, contractors, associates and third-party users understand and carry out their Information Protection Program roles and responsibilities. All employees, contractors, and third parties are trained on their applicable information protection responsibilities and required to attest to their commitment to carry out their information protection roles and responsibilities. Prior to employment, where required, candidates for employment are adequately screened relative to the sensitivity of their job responsibilities. Disciplinary processes are in place and followed when employees and other applicable parties violate the requirements of the Information Protection Program. Responsibilities are in place to ensure that an employee's or contractor's exit from U.S. Bancorp is managed appropriately to ensure ongoing protection of U.S. Bancorp information assets.

New employee orientation addresses information security topics. The onboarding and orientation processes are managed by the Human Resources department. Employees are also required to take information security training within their first 90 days on the job in the U.S. Bancorp online training system. Courses are automatically assigned pursuant to the employee's role, and monitored for completion. Records of completion are stored within the online training system. There are additional courses assigned to those employees who use laptops or other media devices in their role. In addition, any security procedures specific to an employee's position or department are reviewed once on the job.

U.S. Bank conducts pre-employment screening for each applicant that receives a conditional offer of employment, independent contractors and employees of temporary staffing agencies assigned to perform services for U.S. Bank (collectively "new hires"). The decision to hire or not hire an external applicant will be made consistent with applicable legal guidelines and U.S. Bank policy. All new hires must complete a Criminal Background Check as a condition of employment or assignment to U.S. Bank.

There are also approved termination procedures in place. Upon notice that an individual's employment or contract with the Bank has been terminated, managers are responsible for completing all applicable steps outlined in the Termination Checklist for Managers to ensure timely processing of termination. Access to all systems and facilities is promptly removed, and the Human Resources department is also notified.

Security Awareness and Training

U.S. Bancorp's Security Awareness For Everyone ("SAFE") Program establishes U.S. Bancorp's enterprise information security awareness program to provide guidance for the protection of U.S. Bancorp business information, systems and processes to U.S. Bancorp employees, independent contractors and employees of temporary staffing agencies in support of U.S. Bancorp's Information Protection Program. The required courses include specific courses based on an employee's role and access to systems. The training is refreshed frequently. Upon completion of the SAFE courses, employees should be able to understand the U.S. Bancorp information classifications and how to handle information in each classification. U.S. Bancorp's security

awareness program provides ongoing education for all U.S. Bancorp employees and associates on reducing the risk from security vulnerabilities. All new hires, including employees and contractors, are assigned security awareness training on an ongoing basis. An attestation for employees and contractors to acknowledge completion of training is required at the end of the assigned training.

U.S. Bancorp's Code of Ethics and Business Conduct is introduced during new employee orientation and includes information security requirements. Employees are required to complete the Code of Ethics and Business Conduct on-line training after employment and are required to recertify thereafter. The complete Code of Ethics and Business Conduct are located on the U.S. Bancorp Intranet site, and employees are responsible for reading and understanding how the Code applies to them. Employees are also informed of the Ethics Hotline and other reporting mechanisms, such as their manager and Human Resources, if they believe someone is in violation of the Code. All reports made to the Ethics Hotline are reviewed and taken very seriously. Reports may require a formal investigation, concluding with a resolution and/or course of action.

Physical and Environmental

The Company's Information Protection Program has policies with requirements for prevention of unauthorized physical access, damage, and/or interference to enterprise premises and information, including those related to the areas where critical or sensitive information is processed and handled. A Physical Security of Information Assets policy is maintained, approved, communicated, implemented and reviewed.

Physical Access Control

Security perimeters are defined with identification of appropriate access controls. Physical security requirements are commensurate with the identified risks and all critical zones are controlled and monitored via a card access system. U.S. Bancorp has three data centers with active monitoring and security guards on-site 7x24x365. The Security Control Center monitors internal and external data center cameras in real time and retains surveillance videos for 90 days. Any occurrences or incidents on data center property will result in a notification to Corporate Security followed by subsequent investigation and documentation of the event.

Permanent access to restricted areas within buildings is granted only by group assignment and is limited to raised-floor staff, facilities staff and security staff. Any multi-use, multi-tenant buildings grant access to any U.S. Bancorp employee or third party upon manager's request.

Access is managed via access cards or badges and automated card readers. Access reports are reviewed for reconciliation by management. Both permanent and third-party access cards have picture IDs. Other access requests are approved and provided using temporary access cards. Temporary cards, including weekend usages are audited. Visitors are required to sign in and provide appropriate identification before temporary cards are issued.

Equipment Protection

Equipment and information systems are protected from physical and environmental threats. Protection of equipment (including equipment used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage, including storage and disposal. Special controls are designed as needed and required to protect against physical threat, such as the appropriate electrical supplies and cabling infrastructures.

The data centers and hosting facilities have FM-200 gas suppression below raised floors and

Double Pre- Action Sprinkler Systems which are both tested. In addition, portable hand-held fire extinguishers are available above raised floors and are inspected.

Communications and Operations Management

Responsibilities and procedures for the management and operation of information systems are implemented to ensure secure operation of information and information systems. This includes the development of appropriate operating procedures, where necessary. Segregation of duties is implemented, where appropriate, to reduce the risk of negligent or deliberate system and information misuse.

To minimize the risk of system failures and ensure the availability of adequate capacity and resources, operational requirements of new systems are established and tested prior to acceptance and use. System and network controls are required to prevent and detect the introduction of malicious code and unauthorized mobile code. Anti-virus/malware technologies are installed and maintained on end-user computers and servers. Anti-malware software is configured to check for and implement updates at least once per day.

Encryption

U.S. Bancorp encryption standards must support the interoperability of diverse communication systems that handle the storage and transmission of information assets across the distributed environment. Standards must also apply acceptable protocols to meet compliance objectives for PCI standards and Information Security policies.

All websites and applications storing, or processing customer information, use encryption to protect data in transit and in storage, where feasible. Strong encryption must be used to secure the channel to any user's browser. Unknown or untrusted public encryption keys may not be relied upon to provide security. Application session IDs must be encrypted over public networks.

IPS has established processes to manage the renewal of digital certificates utilized by applications for secure communication, where applicable. Digital Certificates used by production applications and services are monitored to remain within their period of validity (i.e. unexpired) and have a trust chain to an IPS-recognized certificate authority.

Network Perimeter Security

U.S. Bancorp uses Intrusion Detection Systems ("IDS"), both network-based and host-based, to monitor for suspicious traffic at trust boundaries. A "trust boundary" is any place on the network where the level of trust to enter a portion of the network changes. IDS passively monitor the network to ensure perimeter firewalls and defenses are effective. Web Application Firewalls are installed on web servers to protect the computing environment from application vulnerabilities.

U.S. Bancorp's IPS Global Monitoring and Detection team and Computer Security Incident Response Team ("CSIRT") partner with a global security services provider to provide 24x7x365 security monitoring and incident response services.

Approved security baselines have been fully documented and provide configuration requirements for all core platforms. Exceptions to the baseline are documented and approved. Secure baselines are updated annually and when the threat landscape changes. To ensure ongoing compliance to the baseline, regular control testing is performed.

Network design is documented to protect critical or sensitive information, and utilizes firewalls with strict rule configurations to control inbound and outbound traffic to U.S. Bancorp network. A formal process is utilized to grant network privileged access to servers and firewalls that includes management approval; this access is reviewed frequently. Firewall administration is performed

using a secure encrypted connection. Firewalls support dynamic packet filtering to monitor active connections and network packets. Firewall configuration is designed to deny all traffic from untrusted networks and hosts. Internet traffic utilizing secure protocols are allowed. Changes to the firewall require authorization and changes are logged. Network logs are securely stored and reviewed regularly by monitoring staff. Network firewall rules are reviewed and updated as appropriate. By default, web filtering blocks personal email sites. Email systems not controlled by U.S. Bancorp (such as Gmail or Hotmail) may only be used for U.S. Bancorp business following approval of a request establishing business rationale. Only individuals authorized to accept risk on behalf of the business line may approve such a request.

Wireless access points to the U.S. Bancorp network are controlled by WPA2 or greater for encryption and authentication. Both the user and machine must be authenticated for U.S. Bancorp network access. In addition, portable automated wireless detection and prevention (WIPS) hardware/software has been deployed to identify prohibited wireless access points and rogue devices on the network. Scans are conducted on wireless accesspoints.

Data Loss Prevention

The Data Loss Prevention (“DLP”) program identifies and protects sensitive data from being shared with unauthorized parties. The DLP program also includes the implementation and application of security policies, procedures, and technical solutions to significantly lower the risk of data leakage.

Portable Electronic Media

PEM includes device types such as CD/DVDs, USB thumb drives, floppy drives and external hard drives with imaging capabilities.

Any distribution of U.S. Bancorp Personal Information on PEM devices to destinations outside of U.S. Bancorp requires explicit approval and instructions from the Privacy Office. All data classified as U.S. Bancorp Confidential or higher must be encrypted with an approved encryption solution when written to PEM devices, regardless of whether the device will remain internal to U.S. Bancorp, or whether the devices will leave U.S. Bancorp premises.

The technology used to enforce PEM controls is currently enabled via a client-server solution. By default, the technology allows Read Only rights to portable media. Access to write/copy data to portable media is granted by assigning the approved Entitlement Role to a user’s security profile for specific types of PEM devices. A user must demonstrate a business need and receive approval to copy data to PEM devices. In the absence of prior authorization, copying data from U.S. Bancorp managed devices to a PEM device is prohibited by policy and prevented by the technical controls described in this section.

Enterprise Information Technology Service Management

U.S. Bancorp maintains an IT Service Management policy that outlines requirements for Incident, Change, Configuration, and Problem Management. The policy covers documentation of changes; request, review and approval of proposed changes; pre- implementation testing; post-implementation testing; review for potential security impact; review for potential operational impact; and rollback procedures.

Access Control

Access to information assets is controlled based on the level of trust of the individual seeking access and the security of the access path. Internal employees and contractors using enterprise-supported computer systems within the network are more trusted than business partners connecting via the Internet; business partners are more trusted than prospective customers; etc.

Access to assets within the network is reduced as the level of trust diminishes.

To ensure information confidentiality, availability, and integrity, access to information resources is provided on a need-to-know and need-to-use basis. Where privileged access is required for those in custodial roles, such as Administrator, access is limited — to the extent possible — to the level needed within the specific custodial role of each individual. Such individuals are educated in and agree to comply with restrictions on their use of privileged authority. U.S. Bancorp uses a centralized provisioning system to manage access requests to high-risk systems, approvals and reviews for end users based on the entitlement assigned (i.e., job function).

U.S. Bancorp has a formal Access Control policy covering physical and electronic records and includes role-based access for all resources, unique IDs for all individuals, restrictions on the use of Generic IDs and prohibits the sharing of IDs and other access devices. U.S. Bancorp uses the centralized provisioning system to set up new accounts and grant access to high-risk systems and resources. When making modifications to user accounts, the manager of the user is required to approve a request to add to or change the user access rights. User access reviews are conducted to validate the appropriateness of user access privileges to systems, applications and networks.

Privileged Access

Privileged accounts and passwords for such accounts are administered and managed internally by an Information Protection Identity and Access Management team. U.S. Bancorp utilizes a privilege account and password management solution for tracking, storing and release of IDs and passwords to authorized teams. The solution ensures that an oversight process exists to monitor and track changes made by accounts with privilege access. It also reduces the likelihood of an administrator using their personal user account to perform updates. Administrative account types include, but are not limited to, emergency IDs, application IDs and service accounts.

Requests for administrative accounts are submitted and approved through the centralized provisioning system. The privilege account and password management solution is designed with segregation of duties and heightened authorization to ensure security. Individuals must be authorized to obtain a privileged ID via multiple approvals.

Password Requirements

A formal password policy prohibits password sharing and requires passwords to be changed at initial log in and at periodic intervals. Passwords are required to be encrypted and/or stored in a location or format which does not comprise the security of the data they protect.

Remote Access

Employees with management approval are permitted to remotely access the network through a secured connection allowed for employees with a business need. Access is granted through an Entitlement Role approved by their manager. Two-factor authentication is required for remote access to the computing environment.

Information Systems Application Development and Maintenance

U.S. Bancorp's Information Protection Program includes requirements throughout the application and system development life cycle (design, development, deployment, maintenance and retirement) to ensure the protection of information assets accessible through business applications. Security requirements for the design and implementation of the information systems supporting the enterprise are identified and agreed upon, where appropriate, prior to the

development and/or implementation of information systems.

The Integrated Delivery Methodology (“IDM”) is utilized for developing, implementing and maintaining securely configured production systems. The IDM is an integrated view of the project delivery lifecycle customized to U.S. Bancorp. It is a set of policies, guidelines, processes, templates and tools defining how projects are planned, managed and delivered.

Delivery (developing, implementing, maintaining) of secure systems to production is ensured by the combined use of the IDM as a foundation, security baselines, and other security services applicable and relevant to the type of system in question. In addition, U.S. Bancorp IPS personnel participate in the Architecture Review and Project Technology Risk Assessment processes to ensure information security requirements and controls are integrated into development and change management processes. Controls and preventative tools have been implemented to ensure that production data does not enter non-production (i.e., test) systems.

Information Security Architecture

U.S. Bancorp’s IPS team works to ensure robust information security architecture. The goals of U.S. Bancorp’s information protection architecture are to provide:

- Defense in Depth
- Enforcement of established U.S. Bancorp policy
- Secure, authenticated access to resources
- Secure deployment of new systems and services
- Secure management of systems, infrastructure and devices
- A logical framework for identifying and investigating security incidents
- Extensibility and flexibility to adapt to changing technology and needs

Incident Event & Communications Management

Appropriate reporting procedures are identified to ensure information security events and weaknesses associated with information systems are communicated allowing timely corrective action to be taken. Responsibilities and procedures are in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement is applied to the response activities and overall management of information security incidents. As necessary, evidence is collected for root cause analysis and extent of damage, to provide a determination of culpability or to comply with regulatory requirements. Throughout this process the integrity of the evidence is maintained to meet forensic requirements. U.S. Bancorp periodically exercises its Computer Security Incident Response Plan in accordance with regulatory requirements and to ensure procedures are adequate to manage U.S. Bancorp’s response to a security incident.

The Global Monitoring and Detection team and CSIRT partner with a Global Security Services Provider to provide 24x7x365 security monitoring and incident response services. The Global Security Operations Center (“GSOC”) is staffed around the clock with qualified information security experts. Internally, U.S. Bank maintains a staff of intrusion detection and Security Information and Event Management (“SIEM”) experts who are on call 24x7x365 to investigate any incidents reported by the IDS or escalated by the GSOC provider.

U.S. Bancorp utilizes several different products to identify intrusion attempts. Standard operating procedures exist to monitor suspicious activity and identify use cases for alerting. IPS has multiple controls in place including, but not limited to, Distributed Denial-of-Service (“DDoS”) monitoring, web log monitoring, IDS, and malware content controls and file integrity monitoring for high risk

systems.

Logs from various security technologies are ingested by the SIEM monitoring tool to alert on anomalies and misuse cases. After an alert is triggered in the SIEM, it is investigated and automatically routed into the security case management tool. A security analyst is assigned to investigate the issue to determine which incident response procedure is applicable, per CSIRT guidelines.

U.S. Bancorp has a team of trained incident response experts and teams dedicated to responding to cybersecurity incidents and events including the following:

- **Global Threat Detection and Event Management:** U.S. Bancorp's 24x7x365 monitoring by security professionals providing first line of support.
- **Global Security Monitoring and Detection:** IPS team of security professionals in charge of system deployment, support, configuration and analysis for security systems and events.
- **Computer Security Incident Response Team:** IPS team of cyber security professionals track down, investigate and mitigate threats.
- **Cyber Intelligence:** A variety of external information sources, including:
 - Subscription information services
 - Memberships in outside security organizations and groups
 - Personal relationships with outside security professionals
 - Participating in information sharing forums such as FS-ISAC
 - Relationships with the Federal Bureau of Investigation, the Department of Homeland Security and other governmental agencies
- **Security Tools:** A variety of software tools used to protect, detect, mitigate, block and analyze threats.
- **External DDoS Services:** U.S. Bancorp uses specialized protection services from internet service providers for large-scale attack detection and mitigation strategies.

Business Continuity and Disaster Recovery

The mission of U.S. Bancorp's Business Continuity Program is to establish and support an on-going Business Continuity and Contingency Planning Program to evaluate the impact of significant events that may adversely affect customers, assets, or employees.

To obtain more information about the Business Continuity Program, you may engage the Enterprise Readiness Services Group through your U.S. Bancorp business line contact.

Compliance

U.S. Bancorp's Information Protection Program aligns with industry-accepted information security practices, where possible, as provided by the NIST Cybersecurity Framework, the International Organization for Standardization ("ISO") and other applicable standards organizations.

In addition, to support U.S. Bancorp's Privacy Policy, U.S. Bancorp's Information Protection Program supports compliance with applicable laws, regulations and contractual requirements. This includes, but is not limited to, the support of compliance with GLBA, SOX, PCI Security Standards and relevant European Union General Data Protection Regulation ("E.U. GDPR") standards.

The Company is subject to review by the Office of the Comptroller of Currency ("OCC"), the

Federal Reserve Board (“FRB”), the Federal Deposit Insurance Corporation (“FDIC”), the Consumer Financial Protection Bureau (“CFPB”), the Securities Exchange Commission (“SEC”), the Financial Industry Regulatory Authority (“FINRA”), among others. In addition to being subject to external regulatory and assessment oversight, U.S. Bancorp also has an internal audit group which serves as a line of defense.

TOS Risk and Compliance organization reports to the TOS Chief Risk Officer and provides oversight to the TOS compliance program.

Corporate Records Management

The Company ensures compliance with data privacy regulations through various compliance policies and procedures. Specific requirements for data/record retention and destruction are stipulated in policies. Retention periods are defined in accordance with the classification of the record. The Corporate Retention Schedule outlines how long records must be retained to ensure compliance with legal, regulatory, and operational requirements. The Corporate Retention Schedule applies to all records that are created and/or maintained by the corporation, including both electronic and paper records.

Several options for secure destruction procedures exist including secure container program, destruction of records stored off-site, destruction of records stored on-site, destruction of plastic and media, and purging electronic records.

Any physical, electronic, and/or media records that have fulfilled the required retention period as defined by the Corporate Retention Schedule must be destroyed. According to U.S. Bancorp information security policies, all records classified as Internal, Confidential, and Personal must be securely destroyed.

Mobile

The Company’s Information Protection Program maintains requirements for secure use of mobile devices and development of mobile device applications to stay current with the evolving technology and use of mobile devices, and to minimize risks inherent with their use. Mobile devices allowed on the network must adhere to documented mobile device policy requirements.

The Company utilizes mobile device management software that enables secure access to information resources such as corporate email, calendar, contacts and intranet browsing on personal and corporate mobile devices. Policies outline acceptable use and oversight procedures when personal or corporate mobile devices are used for storage, processing, or transmission of The Company’s information assets.

Privacy

U.S. Bancorp values the trust placed in it by its customers, and is committed to maintaining that trust by preserving the confidentiality of customer information in accordance with applicable law. U.S. Bancorp is committed to compliance with the U.S. Bank Consumer Privacy Pledge and with GLBA, the Fair Credit Reporting Act (“FCRA”) and other legal requirements relating to privacy, protection and disclosure of customer information.

The U.S. Bancorp Privacy Policy contains requirements for the disclosure of nonpublic personal information. It discusses the types of customer information which may be disclosed and the circumstances under which it may be disclosed. The Policy sets guidelines for the treatment of information that is provided by our customers or collected through any of our online interfaces and our mobile application. The Company’s use and sharing of any information that we collect from or about customers is in accordance with the US Bank Consumer Privacy pledge. For more information about U.S. Bancorp Public

privacy at U.S. Bancorp, please refer to www.usbank.com/privacy.

Software Security

U.S. Bancorp Information Protection Program includes a team of information security professionals dedicated to providing assessment services, penetration testing, application security, mobile security, vulnerability data management, research and analysis and other services that align with NIST Cybersecurity guidance.

Penetration Testing

Testing against all external facing web and mobile applications is conducted to evaluate U.S. Bancorp's exposure to known security vulnerabilities. An application test targets a single application, including the program and its environment components. The operating system, hardware, databases, file systems and network accessibility associated with the application are assessed. The testers apply a variety of attacks against the application to determine whether vulnerabilities are present. Once the assessment is completed, significant findings must be corrected before the application is deployed to production.

Infrastructure testing is performed and includes PCI requirements. Additional testing is executed for new projects, ad-hoc requests and ATM reviews. Testing is conducted internally and by third parties. Retesting is performed to ensure vulnerability closure.

Vulnerability Assessment

Internal and external network scans are performed to identify security vulnerabilities. Scan targets are informed by the Company asset sources of record and checks are informed via plug-ins from the automated tools. Issues identified by security scanning are reviewed for validity and remediated in by working with remediation owners, Technical Owners or system specialists/stakeholders. Response action plans and SLAs are aligned with the risk criticality for remediation prioritization.

Vulnerability Data Management "VDM" processes are implemented to reduce the overall risk of vulnerabilities by monitoring and remediating application vulnerabilities reported and providing support to senior management with consistent and accurate reports.

Vulnerability Data Management (VDM) team's mission includes strategic and tactical focus on peripheral vulnerability responsibilities within U.S. Bancorp and its subsidiaries such as 3rd party scanning on our external network perimeter, results of penetration testing (application vulnerabilities), oversight and analysis of the baseline configuration scanning process.

Additional services include BitSight 3rd party vulnerability management, mobile application vulnerability management, validation of the remediation of risk records, metrics development, reporting, escalation and resolution.

Remediation and Service Level Agreement

Information security vulnerabilities are remediated based on risk prioritization. Issues are classified as Very High, High, Moderate, and Low and remediated within documented SLAs. Documented SLA records for extending remediation may be approved, as necessary.

Patch Management

U.S. Bancorp's security patching and vulnerability management policies require regular patching of software and devices to mitigate the risk of malicious software to U.S. Bancorp environment. Patch Management involves identifying, implementing and validating required patches are in compliance with policies and follow approved processes. To address the potential introduction

of malicious software into the U.S. Bancorp environment, U.S. Bancorp's Information Protection Program maintains requirements for regular patching of software and devices.

Release management processes are implemented to perform reviews that identifies and reports on remediation requirements for potential vulnerabilities on network devices. Testing and Certification processes include test plans and baseline configurations that are vetted by vulnerability scanning in a test environment before submitting for review and approval for deployment to production. Change management processes are implemented to perform upgrades to the environment. Compliance and quality assurance procedures ensure production change requests and upgrades are communicated to engineering teams to ensure consistency with published standards.

The process for applying updates to workstations involves reviewing industry patch release notifications that are published for computing platforms. Configuration reporting tracks successful patch implementation with metrics and other data that are used to communicate requirements to technical teams for remediation.

Servers patching process include reviewing and identifying industry patch release notifications, running scans, testing patch solutions, and deploying applicable patch through change management processes. Compliance reports are updated with data regarding the most current patching information. Validation reports with data on patch compliance results are reviewed by technical teams to confirm successful implementation and remediation activities.