Family First Credit Union
Change Management Procedures

Information Systems Change Management Standards

Family First Credit Union acquires its technology systems and application software from third party technology vendors. For example, the Credit Union's core processing system (e.g. deposit, loan, and general ledger accounting systems) were acquired from Fiserv. These systems are primarily maintained by the vendor from whom they were purchased. In most cases, Family First Credit Union does not have possession of source code to make changes; however, the Board of Directors and management are aware that:

- Vendors make periodic changes to application software used by the Credit Union, including comprehensive changes in the form of new releases and "fixes" of immediate problems.
- The Credit Union has the option of changing parameters, options, etc. which alter the functions of specific applications.

Further, the Board and management understand that either of these categories of changes may affect the effectiveness of the Credit Union's Information Security Program. Consequently, any change to the Credit Union's systems, application programs, computer hardware, and data communications hardware and software may impair the effectiveness of Family First Credit Union's Information Security Program. Consequently, these standards have been adopted to provide guidance for managing such changes.

Software Change Control

Software change control covers the control of all aspects of critical systems software including the operating systems, compilers, utilities, and third party and in-house developed applications together with any command procedures and documentation to support and run them.

General Obligations

When software changes are required, it is essential that the changes are appropriately authorized and approved. Authorization for any software change must come from the Change Advisory Board (CAB). Exceptions will be made for changes intended to correct errors or security vulnerabilities found in existing programs or procedures and for "patches" to existing systems such as Program Temporary Fixes (PTF) or Service Packs (on network systems). Because it may not be prudent to delay applying such changes while awaiting approval, these changes are permitted. All requests will be made via the FFCU Helpdesk Ticketing system. All Change Management requests will be documented in the FFCU Helpdesk system.

All software changes will adhere to the following guidelines:

- They may not violate existing policies or procedures.
- They must be tested in a separate environment (when applicable).

- They must be documented.
- Any software changes that disrupt member activities, credit union workflow, or system operations must be implemented during established maintenance windows, typically outside of hours of operation.

Change Request Requirements

Any of the following requests will require submission of a change request to the IT Department:

- Initiate a new information processing capability.
- Alter an existing processing capability.
- Alter a system profile.
- Repurpose an existing information product.
- Alter an existing information product.
- Create a new information product.
- Flaw Remediation reporting.

The change request for an existing information product or process must contain all relevant documentation to justify the scope of the change which may include one or more of the following:

- Description of current information product or process.
- Description of why the current information or process needs to be changed.
- Anticipated outcome if the change is made.
- Value to the Credit Union if the change is made.
- Risk to the Credit Union if the requested change is not made.
- Impact to the existing information product or process in affecting the change.
- Impact to other related information product or process in affecting the change.
- Time frame in which the change request must be completed.

The change request for a new information product or process must include the following information:

- Description of the new information product or process.
- Description of why the new information product or process should be implemented.
- Anticipated outcome of the new information process or product.
- Value of the new information process or product to the Credit Union.
- Risk to the Credit Union if the requested new information process or product is not implemented.
- Impact on existing information product or process in implementing the new information process or product.
- Impact on budget.

Change Advisory Board (CAB) Members

- Kimberly Echols, Chief Operations Officer
- Wanda Norman, VP of Compliance
- Wayne Pike, VP of Information Technology Department
- Daniel Large, Information Technology Specialist

Change Consideration and Approval

Change control requests will be evaluated by the Change Advisory Board. The change request will be evaluated for:

- Resources required to implement the change request.
- Cost of implementing the change request.
- Impact on other collateral or cost centers such as user manual or other documentation, training, and Service Desk support.
- Time required and schedule for implementing the change request.
- Testing environment and testing requirements for implementing the change request.

Change Control Environment

Software changes will be implemented through the utilization of three separate steps to the degree it is economically feasible and practical:

1. Development – New program releases or significant program changes are typically prepared by a third-party service provider. The Credit Union does minimal programming except for custom report generation.
2. Testing – Once a program changes or new release is received from a vendor, it must be thoroughly reviewed by the VP of IT and appropriate, designated end users. The purpose of such review is to determine the effects of the proposed changes on the Credit Union's information security systems and on the operational systems. The IT Department will ensure that the implementation of the new release or program change will not materially impair the effectiveness of the Credit Union's information security systems.
3. Production - This is the environment in which the current, active software resides. Only after a program has completed the testing phase satisfactorily and has been approved may it be moved to the production environment. Results will be documented with a Service Desk ticket. Once testing is completed, the ticket will be closed, and the system will be moved into production.

Network Changes

Only changes approved by the Change Advisory Board, including emergency changes, may be made to the Credit Union's networks. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems. This applies to vendor personnel as well as Credit Union personnel. Network change requests will be made via the FFCU Helpdesk Ticketing system. All Change Management requests will be documented in the FFCU Helpdesk system.

Hardware Installation

Installations of hardware at the Credit Union typically involve two types of devices: a) non-cash devices (computers, printers, monitors, network hubs, modems, routers, etc.), and b) cash devices (ATMs, cash dispensing machines, etc.). The following guidelines will apply to hardware installations:

Non-Cash Devices

Non-cash devices may be installed at any time; however, installations must be approved by the President/CEO and coordinated with the IT Department and the department/branch manager. If the installation takes place behind the teller line, in the vault area, or any other cash handling area, the installer must be accompanied by a branch representative. Installations that take place outside of cash handling areas or after business hours when no cash is present may be completed without a branch representative in attendance.

Cash Devices

A credit union representative must always accompany the installer when cash is present. The following steps must be taken when installing a cash device:

- Establish the requirements and actions for the installation:
  - The actions to be completed prior to installation.
  - Installation day actions.
  - Post installation follow-up.
- Ensure that branch colleagues have been trained on the equipment.
- Verify with the Financial Accounting Department that all GLs are in balance.

Under no circumstances is the installer to be allowed or required to handle cash.

Hardware Standards

All hardware acquired, including computers and peripherals, must meet reputable industry standards. When possible, standard brand names will be used to allow for continuity of products, availability of maintenance, and an adequate supply of replacement parts. Any new purchases must be approved by the President/CEO and will be subject to certain minimum standards. These standards are subject to change by the IT Department due to technology and/or cost changes.

Personal Hardware

In order to limit Family First Credit Union's exposure to malicious code and other harmful consequences, *absolutely* no personally owned hardware will be installed on the Credit Union's local area networks, wide area network, or credit union-owned computers without prior authorization of the VP of IT. Unauthorized modifications made to systems may be viewed as a breach of security and require an incident response.

Software Licensing and Copyright

Each individual user will use only legally obtained *and pre-approved* software on the Credit Union's computing equipment. Users will be held liable for any breach of copyright. Users should become familiar with the restrictions placed on their license. (If you need assistance understanding the license agreement, contact the IT Department). The IT Department serves as

the custodian of all software licenses at the Credit Union. The Credit Union will not be liable for any copyright violations traceable to users or undocumented installations.

Software in the possession of the Credit Union must not be copied unless such copying is consistent with relevant license agreements and the VP of IT has previously approved such copying or copies are being made for contingency planning purposes. **Unauthorized use, duplication, or reproduction of Credit Union-owned software is strictly prohibited**. Pirating software (the act of illegally using, copying, or distributing software without ownership or legal rights) is a felony punishable by state and federal laws. Violators of these standards are subject to suspension or dismissal.

Software Security

Credit Union software, accompanying documentation, and all other types of internal information must not be sold or otherwise transferred to any party outside of the Credit Union for any purposes other than those explicitly expressed and authorized by the President/CEO.

Exchanges of software and/or data between the Credit Union and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange as well as the ways in which the software and/or data is to be handled and protected. Regular business practices (such as shipment of software in response to a customer purchase order) need not involve such a specific agreement since the terms are implied.

Software Purchase, Upgrade, and Installation

The IT Department evaluates requests for software purchases or upgrades considering product/version standardization.

- All software must be installed by or under the direction of the IT Department.
- No personal software will be installed on credit union-owned computers.

Software Support

The IT Department supports sanctioned software only.

Software Documentation

We define documentation as the written material that describes:

- Evidence of ownership/rights (e.g., license, contracts, programming, etc.).
- The user's manual or operational procedures to run the program.
- Any other information needed for someone else to understand how to use the program.

This documentation will be maintained with the software in the department where it is used or in the IT Department.

All purchased software must be documented with a copy of the documentation kept in a secure area unless management specifically approves a purchase without such documentation. All

software documentation licensed to the Credit Union must include appropriate copyright notices. Documentation must also reflect any changes occurring from software releases or updates.

Personal Software

The use or installation of personal software on credit union-owned computers is prohibited. Examples include, but are not limited to, games, screen savers, utilities, and background software.

The IT Department will periodically perform a sampling audit of computers to ensure compliance. If unauthorized applications are detected, they will be removed from the computers without notice and the offender's manager will be notified.

Operating Systems

A review of all existing operating systems is conducted on a daily basis by the IT Department using several systems including BelManage and WSUS server along with Solar Winds Patch Management to check for upgrades, releases, and patches that may recently have been made available. This includes network operating systems, individual desktop operating systems and software, mobile device operating systems, email operating systems, proxy server operating systems, network backup and recovery systems, and the host processing system. The changes made within these upgrades are examined to determine the urgency of the need to apply the modifications.

If a problem occurs that requires a patch to be installed outside the regularly scheduled times, the IT Department will apply the necessary updates, document the activity in BelManage and notify the President/CEO or VP of IT.

Whenever possible, upgrades, releases, and patches will be scheduled for implementation during off-peak hours. All installations must be performed by or under the direct supervision of the IT Department.

The IT Department is also responsible for installing and updating desktop operating systems, office automation software products, email clients, network clients, browser software, various product clients, and other software used at the desktop level. These updates are performed on an as-needed basis.

Every effort is made to maintain consistency throughout the network, but because of user preferences and the number of computer systems in use, it is not possible to always have the same exact levels of software on every computer. As new computers are introduced and older computers are reloaded, the latest licensed software and software updates are always applied. Using several systems including Microsoft Windows Server Update Service, BelManage, Solar Winds Patch Management, the IT Department will ensure that appropriate security patches are installed on all devices within the Credit Union.

Core Processing System (CUnify) Software HOSTED

Fiserv provides the Credit Union software updates and installations done via hosted database. Because of the potential wide-ranging impact of these software releases, the scheduling, training, and implementation of the release is more complex than with operating system software when the changes are usually transparent to the user.

The following outlines the basic steps performed when core software release has been made available to Family First Credit Union:

- Prior to loading a release in the production server, a list of all software changes is emailed to the Operations Department and the IT Department.
- If the COO and the VP of Information Technology finds that there is a need for training, they will schedule such training with all colleagues, or they will train the trainer. This is especially true if the software includes a new process.
- The actual release installation must be scheduled far enough in advance so that all colleagues are properly notified. Fiserv will be notifying the Credit Union of the release installation date.
- If the release includes any pre-installation tasks, they will be completed at least one week prior to the release installation if possible.
- All colleagues are notified of any process changes that this release may include.
- If the release notes indicate third-party programs will be impacted by the release they will be tested for compatibility. Any failures will immediately be reported to Fiserv.
- Updated manual documentation will be distributed to the appropriate departments/branches.
- The first processing cycle following the installation of the release will be closely monitored by the appropriate departments to make sure that all changes were implemented as expected and no existing processes were negatively affected.

System Hardening Checklists

The first step in securing a system (server, computer, laptop, etc.) is securing the underlying operating system. To assist in ensuring the Credit Union's systems are protected, the IT Department will establish system hardening checklists. Once a checklist has been written, it will be tested and validated to ensure consistent secure system deployment.

The IT Department may create its own checklist procedures or work from a template provided under the National Checklist Program[1] or another reliable source.

A checklist may include the following items as determined by VP of IT:

- Configuration files that automatically set various security settings (standard XML format such as that utilized in Security Content Automation Protocol (SCAP),[2] executables, security templates that modify settings, and scripts).

[1] The National Checklist Program defined by NIST SP 800-70 Revision 2, is the U.S. government repository of publicly available security checklists that provide detailed, low level guidance on setting the security configuration of operating systems and applications and can be found at http://web.nvd.nist.gov/view/ncp/repository.

[2] NIST's Guide to Adopting and Using the Security Content Automation Protocol (SCAP) version 1.2 (draft) can be found at

- Documentation (for example, a text file) that instructs the checklist user how to interactively configure software to recommended security settings.
- Documentation explaining the recommended methods to securely install and configure a device.
- Policy documents that set forth guidelines for such things as auditing, authentication security (for example, passwords), and perimeter security.

Operating Systems

Securing an operating system prior to adding the system to the trusted computing environment (LAN) generally includes the following steps:

- Ensuring the operating system has the latest patches and upgrades. If not, patches and upgrades will be reviewed for their applicability to the Credit Union's environment and installed as needed.
- Removing or disabling unnecessary services, applications, and network protocols.
- Configuring operating system user authentication.
- Configuring resource controls.
- Installing and configuring additional security controls if needed.
- Installing antivirus software.
- Performing security testing of the operating system.

Server Applications [3]

To mitigate the risk associated with unused portions of the software and possible vulnerabilities that may exist, it is the responsibility of the IT Department to "harden" software before deployment by:

- Ensuring accessible applications have the latest patches and upgrades. If not, patches and upgrades will be reviewed for their applicability to the Credit Union's environment and installed as needed. (Application-level exploits are extremely popular, so this is very important!)
- Determining the purpose of the system and minimum software and hardware requirements.
- Documenting the minimum hardware, software, and services to be included on the system.
- Installing the minimum hardware, software, and services necessary to meet the requirements using a documented installation procedure.
- Removing or disabling unnecessary services, applications, and sample content.
- Configuring privilege and access controls by first denying all, then granting back the minimum privilege and access controls necessary to each user.
- Configuring security settings as appropriate, enabling allowed activity, and disallowing other activity.
- Enabling logging.

http://csrc.nist.gov/publications/drafts/800-117-R1/Draft-SP800-117-r1.pdf.

[3] NIST's Guide to General Server Security can be found at http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf.

- Testing the system to ensure a secure configuration.
- Changing all default passwords.
- Testing the resulting systems.

Patch Management

The Credit Union's computers must be properly patched with the latest appropriate updates to reduce system vulnerability and protect the entire network from malicious attack. The purpose of this standard is to establish procedures for the identification of Credit Union system vulnerabilities as well as the safe and timely installation of vulnerability patches.

The IT Department will be responsible for maintaining an effective patch management process. Specifically, the patch management process will ensure all available patches are reviewed and installed when applicable. Documentation will include decisions to install or reject specific patches. Patches will be installed in a test environment for an impact assessment when deemed necessary by the IT Department. The patch management process will cover operating systems, core processing systems, business applications, and system services. The necessity of patch implementation will be weighed against downtime impact for scheduling the installation and will generally be installed/applied after normal working hours. Monthly assessments performed by the IT Department will include the effectiveness of the patch management process and evaluate whether previously rejected patches should be installed.

This standard applies to all servers, computers, and laptops owned and operated by the Credit Union.

- Only designated individuals will perform vulnerability assessment and system patching.
- All server, computer, and laptop systems, including all hardware and software components, must be accurately listed in the IT Department asset inventory to aid in patching efforts.
- Each vulnerability alert must be checked and tested against existing Credit Union's systems and services prior to taking any action to avoid unnecessary patching. Read all alerts very carefully – not all patches are related to vulnerability issues or actual system versions present at the Credit Union.
- All patches must be downloaded from the relevant system vendor or other trusted sources. Each patch's source must be authenticated, and the integrity of the patch verified.
- New servers and computers must be fully patched before coming online to limit the introduction of risk.
- All patches must be tested prior to full implementation since patches may have unforeseen side effects.
- A back-out plan that allows safe restoration of systems to their pre-patch state must be devised prior to any patch rollout if the patch has unforeseen effects.
- All configuration and inventory documentation must be immediately updated to reflect applied patches.
- Audits will be performed to ensure that patches have been applied as required.
- The IT Department will maintain evidence of its patch management efforts within the automated patch management solutions (Solar Winds Patch Manager and WSUS) employed by the Credit Union.