Xtend
Policy Manual

2021

6000 28th St. SE, Grand Rapids, MI 49546 | (866) 981-4983 | info@xtendcu.com | xtendcu.com
This Policy Manual is intended to provide requirements for continued employment with Xtend. These policies are dynamic and under constant review. Policies currently in effect may be revised, suspended, or eliminated by Xtend in response to changing marketplace and/or legal requirements.

Any changes to this manual will be communicated to staff. Some policies are necessary due to company compliance requirements with federal or state laws. If a question ever arises about the nature and extent of Xtend policies and any conflicts with regulations, the requirements of the specific laws or regulations govern.

**WARNING**

*Failure to adhere to policies may result in discipline up to and including termination. Willful violations of policies which are also violations of law may result in fines, imprisonment, or both.*

None of the policies included in this manual are intended to, nor do the policies grant, any contractual rights. This policy manual may be amended or revised from time to time as the need arises. The policies in this manual supersede any contrary or previous versions.
### Contents

1. **CALL CENTER POLICY** .................................................................................................................. 8
   - Rules of Engagement (ROE) ........................................................................................................... 8
   - Call Flow and Scripts .................................................................................................................... 8
   - Challenging Calls .......................................................................................................................... 8
   - Escalation ......................................................................................................................................... 8
   - Telephone Regulations ................................................................................................................... 8
   - Large Scale Absence ...................................................................................................................... 8
   - Communication .............................................................................................................................. 8
   - Additional Pandemic Policies ........................................................................................................ 8

2. **RELEASE OF RECORDINGS** ........................................................................................................ 9
   - Phone Recordings ........................................................................................................................... 10
   - Quality Control Monitoring .......................................................................................................... 10
   - Designated Users ............................................................................................................................ 10

3. **RECORDING PROCESS** ............................................................................................................... 11
   - Monitoring Process ....................................................................................................................... 11
   - Employee Coaching ....................................................................................................................... 12
   - Records ........................................................................................................................................... 12
   - Administration ............................................................................................................................... 13
   - Client Access to Recordings ........................................................................................................... 13

4. **POLICY PURPOSE AND OVERVIEW** .......................................................................................... 14
   - Sensitive Information Defined ..................................................................................................... 14
     - Nonpublic Personally Identifiable Financial Information (PIFI) ................................................. 14
     - Sensitive Employee Information ................................................................................................ 14
     - Confidential Client and Vendor Data ............................................................................................ 14
     - Trade Secrets and Confidential Employer Information ............................................................... 14
     - Consumer Privacy ....................................................................................................................... 15
     - Confidential Client Information .................................................................................................. 15
     - Private Information of Members and Non-Member Customers of Clients ............................... 15
     - No Obligation to Protect Publicly Available Information .......................................................... 15
     - Employee Bond ........................................................................................................................... 15
Minimum Requirements for Data Security ................................................................. 15
Use Encryption ........................................................................................................... 15
Ensure Authorization ............................................................................................... 15
Do Not Disclose Unless Authorized ........................................................................ 16
Store Sensitive Information Securely ........................................................................ 16
Data Leakage ............................................................................................................. 16
Notify When Suspected Security Incident Occurs .................................................... 16
Destroy Sensitive Information Securely ...................................................................... 16
Passphrases and Passwords ...................................................................................... 16
Building Security Requirements ................................................................................ 16
Sign in for Access ...................................................................................................... 16
Secure Access ........................................................................................................... 16
Badge Colors and Access ......................................................................................... 17
Visitor Access ........................................................................................................... 17
Keyfobs ..................................................................................................................... 17
Access by Landlord(s) and Security Contractor ......................................................... 17
Building Alarm Access ............................................................................................. 17
False Alarms .............................................................................................................. 18
End of Day Protocols ............................................................................................... 18
Employee Separation ............................................................................................... 18
Security Cameras ....................................................................................................... 18
Social Engineering Avoidance .................................................................................. 18
3. INFORMATION SECURITY POLICY AND PROGRAM ............................................. 20
Policy Purpose and Overview .................................................................................... 20
Data Classification .................................................................................................... 20
Program Implementation .......................................................................................... 21
Risk Assessment ....................................................................................................... 21
Manage and Control Risk ........................................................................................ 21
Security Breach ......................................................................................................... 21
Incident Response Protocol ...................................................................................... 21
5. LARGE SCALE ABSENCE POLICY .................................................. 31
   Large Scale Absence Program .................................................. 31
   Methodology ........................................................................... 31
   Client Serving ......................................................................... 31
   Coverage of All Shifts ............................................................. 31
   Prioritizing Daily and Pending Duties ..................................... 31
   Managing Project Timelines .................................................... 31
   Delivery .................................................................................. 31
   Handling the Essential Duties ................................................ 31
   Operations .............................................................................. 31
   Cross-Departmental Coverage ............................................... 31
   Travel During Event ............................................................... 32
   Additional Pandemic Policies .................................................. 32

6. RECORDS POLICY AND LITIGATION HOLD .................................. 33
   Scope and Definitions .............................................................. 33
Principles .............................................................................................................................................. 33
Internal Records Only .......................................................................................................................... 33
Preserve Only Records of Value .......................................................................................................... 33
Establish Safeguards ............................................................................................................................ 33
Responsibility of Owner/Creator ......................................................................................................... 33
Retention Schedule ............................................................................................................................. 34
Litigation Hold ...................................................................................................................................... 34

7. VEHICLE POLICY ............................................................................................................................. 35
Definitions ............................................................................................................................................ 35
  Company Vehicles .............................................................................................................................. 35
  Rental Vehicles ................................................................................................................................. 35
  Company Business ............................................................................................................................ 35
  Driving Related Position ................................................................................................................... 35
Scope ................................................................................................................................................... 35
Eligible Drivers .................................................................................................................................... 35
Driving Record Criteria ....................................................................................................................... 36
  Good Driving Records .................................................................................................................... 36
  Violations ......................................................................................................................................... 36
Acceptable Use of Vehicles .................................................................................................................. 36
Driver Safety Rules .............................................................................................................................. 36
Maintenance of Vehicles ...................................................................................................................... 37

8. VENDOR MANAGEMENT POLICY ................................................................................................ 38
Vendor Management Program ............................................................................................................. 38
Oversight .............................................................................................................................................. 38
Vendor Risk Oversight ........................................................................................................................ 38
  TIER I ............................................................................................................................................... 38
  TIER II ........................................................................................................................................... 38
  TIER III .......................................................................................................................................... 39
  TIER IV .......................................................................................................................................... 39
  TIER V ........................................................................................................................................... 39
Evaluation Process ............................................................................................................................... 39
Evaluation Reporting ............................................................................................................................ 40
1. CALL CENTER POLICY

Rules of Engagement (ROE)
All credit unions shall provide Xtend with Rules of Engagement (ROE) for Xtend call center employees. In the event a credit union ROE conflicts with Xtend policies, the ROE has overrides and supersedes Xtend policies.

Call Flow and Scripts
Xtend will provide Call Flow and Call Scripts to guide employees on how to answer calls, call backs and tracking of calls. In addition, guidance will be provided on transferring calls to the credit union.

Challenging Calls
When dealing with a difficult call, employees shall remain professional at all times and inform callers that staff will do their best to assist in resolving the request. If an employee encounters a caller who demonstrates threatening, aggressive, belligerent, or other clearly inappropriate behavior or language. Employees will calmly inform the caller that continued inappropriate behavior will result in a termination of the call.

Escalation
The Processing Guide determines the procedure for escalation. Managers can be brought in through Instant Messaging or by placing the caller on hold and asking for assistance.

Telephone Regulations
Xtend adheres to all applicable and enforceable federal and state laws and regulations governing outbound telephone calls for the protection of the privacy of telephone consumers.

Large Scale Absence
A large-scale absence, for purposes of this document, is defined by Xtend as missing 50% or more of the employee population for a period of up to two (2) consecutive weeks. The determination that Xtend is experiencing a large-scale absence event will happen at the Corporate Officer level. Delays in servicing our clients should be expected. Clients will be contacted appropriately by sending out a scripted message using our emergency response text platform. Management must assist employees to prioritize the workload.

Communication
If Corporate Officers declare a large-scale absence event has occurred at Xtend, clients shall be notified via the Emergency Notification System.

Managers will be responsible for communicating to their staff members any new priorities or changes in responsibilities resulting from the event.

Additional Pandemic Policies
If the absence is due to a pandemic disease, the following additional controls are required: infected staff should defer coming to work for the length of the incubation period of the virus; staff should utilize the hand sanitizing stations provided around the office and wash hands.
often; clean keyboards and other equipment, especially if workstations are shared between staff members; a certain degree of social distancing could be practiced; reducing frequency, proximity, and duration of contact can also help reduce the spread.

Staff interactions during an event will be decided upon by Xtend Corporate Officers and communicated to the employees through ORD. Depending on the circumstances surrounding the event, decisions will be made regarding: severely discouraging or disallowing large assemblies of employees (on or off work premises); closing all meeting rooms; limiting all staff interactions as much as possible; encourage or force employees to work at home or at other Xtend offices; and/or offering masks and setting up for cleaning stations around the office.

**Release of Recordings**

Release of phone call recordings shall be in accordance with Xtend's Call Release Protocol, as detailed on the following page.
Protocol for Quality Control Review and Release of Phone Recordings

For Distribution to All Clients

Phone Recordings
Xtend records phone interactions between certain Teams and clients, and also directly with credit union members for certain services. We use the Current system for recordings. The purpose of the call monitoring program is to make sure that employees are facilitating the best possible customer experience for our clients and their members.

The call recording process at Xtend is applied to client facing staff under the supervision of the Xtend CEO for the improvement of our customer service to our Partners, Clients and their Members.

Control of the call recording process at Xtend is achieved through administration of the software categories by Internal Networks with oversight of the current Phone System Program applications by Organizational Resource Development.

Quality Control Monitoring
Our company maintains a scoring guideline that gives the observer the ability to compare behaviors that are detected during calls against a preset standard. The closer the employee’s actions are to the standard the higher the quality score will be and vice versa.

Although the scoring system is not a perfect measure for what constitutes ideal client interactions, it does provide a guide for acceptable and expected behaviors from the organizational level. Employees should be able to concentrate on the reason for the call while still meeting the basic guidelines.

There are three primary goals to the process: provide feedback and specific coaching to employees on phone call performance; improve/maintain the professional image of Xtend and its partners in all client interactions; and provide corporate risk management with regards to client interactions across the organization.

All calls received and placed by designated users within the Phone System are recorded and subject to monitoring, this includes calls forwarded to personal phones from within the Phone System. Calls and communications routed through the Phone System are also subject to recording and monitoring.

Designated Users
A designated user is defined by the employee’s position and/or based on management request. Designated users are recognized within the phone system by their network login information no matter which workstation they may be logged into. If a user is logged into a workstation with his/her network login, then all phone calls received and placed by that user will be recorded:
• All internal calls from or to a designated user within the phone system are recorded, even if the other caller is not a designated user.

• All external calls from or to a designated user within the phone system are recorded.

• Calls forwarded by a designated user to a “follow-me” number (cell phone, home phone, other extension) will be recorded for the duration of the call (even when the call is picked up on the other communication device.)

• Calls transferred from a designated user to a non-designated user will only record up to the moment when the transfer is made to the new extension.

• Break Room phones (and other phones not attached to workstations) are not recorded, however, if someone makes a call from the break room to a designated user that call will be recorded. If a designated user goes to the break room to make a call to a family member outside the organization the call will not be recorded.

• All employees have waived their right to privacy when utilizing the company phone system as outlined in the Employee Handbook.

**Recording Process**
The call recording process is conducted via the Phone System and securely contained within Xtend’s phone network and servers. All calls for designated users are recorded for quality control purposes. Each call is identified using a unique call identification code, then encrypted and kept for a length of 90 days. The recorded and stored files are automatically purged after 90 days.

**Monitoring Process**
The selection of calls to be monitored and scored as required by this procedure is intended to provide a sampling of phone interactions performed by individual people. Each call in the sampling is intended to be scored for basic phone skills performance. The sample is then assessed for performance strength and weakness of the individual. Calls that score significantly below or above the Standard will be identified for call coaching.

Call recordings, both external and internal, are selected from the system, scored, and recorded on an individual scoring sheet. The scoring sheet outlines the basic guidelines for quality customer service of the organization which fit within the customer service performance areas of:

• Greeting skills where the employee is expected to greet the client; identify themselves and find out why the client is calling.

• Customer service skills where the employee provides quality client service based on specific areas of listening, communication, understanding the request and successfully helping the client.
• Procedural requirements where the employee follows the organizational expectations for specific procedures such as contact verification, holds, transfers and documentation.

• Closing skills where the employee is expected to wrap up the conversation positively.

Each skill is scored based on the performance of the employee in that particular area. Skills are weighted differently with the customer service skills area having the heaviest weighting. The goal of this procedure is to guide team and individual performance to provide excellent customer service to our clients and our clients’ members through employee skill coaching and development.

Summary reports of all monitored phone calls will be compiled monthly for review by the managers of each department. Average performance scores are reported by individual and by department. Any scores above or below standard are identified so management is aware of strengths and weaknesses on their team and address them as necessary. Management contributes to the monthly report by logging the calls they monitored and scored for their department and by indicating the individual coaching sessions they had with employees.

Unprofessional or inappropriate incidents identified during observation are immediately reported to the appropriate manager for mandatory coaching and/or disciplinary actions as determined necessary.

System Workgroups are audited for appropriate membership annually. Change Forms are completed as necessary and submitted to Internal Networks to make requested changes to a Workgroup. An appraisal of this procedure will be assessed periodically with revisions implemented when warranted.

**Employee Coaching**

Calls can be identified for coaching purposes by either the Client Services Quality Coordinator or department management. The call scoring form is used in conjunction with an audio recording of the call to coach the employee on specific calls. Managers are encouraged to conduct and document real-time employee call performance or in the event of an incident or issue identified by management.

Upon completion of a mandatory coaching session, management and the coached individual sign and date a hard copy of the call scoring form.

**Records**

Records of the monthly call monitoring and employee coaching activities are retained for review and auditing purposes. Call monitoring reports are maintained by Xtend. Electronic records of call monitoring reports and recordings are retained for 90 days. Electronic records of individual call monitoring forms and recordings are retained for 90 days. Records of performance write ups for call coaching are retained in hard copy format by Organizational Resource Development for a minimum of one year. Records of mandatory coaching sessions are retained by Organizational Resource Development indefinitely.

Call recording responsibility affects three facets of the Xtend organization. Administration of the current Phone System Program is carried out by Internal Networks with oversight of current Phone System applications conducted by Organizational Resource Development and utilization of the Current Applications made by departmental management within Xtend.
Administration

CU*Answers Network Services (CNS) maintains the current Phone System Program which operates through unified messaging conducted between our Microsoft Outlook Program and the current Phone System Program to enable phone recording on our telephone system. CNS controls all Interactive Intelligence Program Applications; license allocation, category configuration, access and control assignments within the current Phone System Program.

Current System users are assigned appropriate Program Application licenses, categories and accesses by CNS at the direction of Xtend management through the workflow contained in Passageways. Category configuration by CNS establishes rules for recordings that affect which employee’s calls are recorded, which employees have the ability to listen to recorded calls and which employees have access to recorded call data reports. User changes to the current Phone System Program are requested by management submitting a Change Form for review and appropriate implementation of the change.

Change Form requests are submitted to CNS for implementation. Department management determines the call recording needs within their area of control. Additions or changes to the departmental call recording needs are made by submitting a Change Form requesting the appropriate program application or configuration change. Management and supervision of any Interactive Intelligence Application used for call recording purposes within the department is carried out by authorized management personnel.

Client Access to Recordings

Upon request, Xtend may provide a transcript of the conversation or play the recording over the phone for the client to review. The request must be made prior to 90 days of the call to guarantee that the recording will be preserved. Teams will not provide a copy of the call monitoring reports, or report of any internal discipline as the result of a call interaction. Clients may not request a copy of a recording.
2. CYBERSECURITY POLICY

Policy Purpose and Overview
Employees and contractors have a duty to safeguard sensitive information. Sensitive information includes trade secrets, confidential or proprietary information of Xtend, its partners or clients, and the non-public personally identifiable financial information of credit union consumers or members, as well as the employees and contractors of Xtend.

Every Xtend employee and contractor is responsible for ensuring that use of Computer Resources, as well as outside computers and networks, such as the Internet, does not compromise the security of Xtend. This duty includes taking reasonable precautions to prevent intruders from accessing the company’s network without authorization, preventing introduction and spread of malware, and the use of other reasonable means to protect sensitive information.

Employees and contractors must take reasonable steps to ensure sensitive information is maintained and transmitted securely. Employees and contractors must not disclose sensitive information unless authorized by job description or by an officer of Xtend.

WARNING
In addition to discipline up to and including termination, willful violations of policies that are also violations of law may result in fines, imprisonment, or both.

Sensitive Information Defined
Nonpublic Personally Identifiable Financial Information (PIFI)
This includes information that can be linked, directly or indirectly, to individual consumers of financial products, per Regulation P (Sections 502–509 of Title V of the Gramm-Leach-Bliley Act). Examples include, but are not limited to, Social Security numbers, credit union account numbers, and credit and debit card numbers that can be identified to a financial consumer.

Sensitive Employee Information
This includes, but is not limited to, health records, payroll records and other non-public personal records of Xtend employees and contractors.

Confidential Client and Vendor Data
Xtend has agreements with our clients and vendors promising to secure their confidential information. Generally speaking, confidential client or vendor data is any data regarding client or vendor business that is not known or available to the public.

Trade Secrets and Confidential Employer Information
Trade secrets and confidential employer information includes information protected from disclosure through Xtend’s reasonable efforts to maintain its status as a “secret.” Xtend’s confidential data and trade secrets may include but is not limited to: proprietary computer software programs; proprietary databases, business processes and methods; information pertaining to overhead, costs, pricing and margins; strategic plans; and marketing programs.
Consumer Privacy
Xtend is required to have a high standard of care regarding the confidential information of our clients and their consumers or members. This policy describes Xtend policies towards both confidential client information and the nonpublic personal information of credit union member and non-member customers.

Confidential Client Information
Xtend will not use or disclose to any third party any information concerning the trade secrets, methods, process or procedures or any other confidential, financial or business information of a client which it learns during the course of service. Xtend will treat client information with the same degree of care that it treats its own most confidential information and shall disclose such information only to employees or representatives who require such in the ordinary course and scope of their employment.

Private Information of Members and Non-Member Customers of Clients
Xtend intends to protect the privacy and confidentiality of nonpublic personal information of the members and non-member customers of any Credit Union Xtend has an agreement with. Xtend is prohibited from disclosing or using nonpublic personal information about the Credit Union’s members other than to carry out the purposes for which the Credit Union disclosed the members’ nonpublic personal information.

Xtend shall disclose to the Credit Union any breach in the security resulting in unauthorized intrusions into Xtend’s systems that may materially affect the Credit Union or its members.

No Obligation to Protect Publicly Available Information
Xtend has no obligation to protect information which (i) was publicly available or in the public domain at the time of disclosure, (ii) becomes publicly available or in the public domain subsequent disclosure through no fault of Xtend, (iii) free of any obligation of confidence to the disclosing party at the time of disclosure, or (iv) is disclosed to Xtend from another source rightfully possessing it.

Employee Bond
Xtend agrees that any of its employees who have access to internal information or Credit Union information will be sufficiently bondable against fraud or other dishonesty.

Minimum Requirements for Data Security
The following are the core rules with respect to the use and protection of sensitive information:

Use Encryption
Employees and contractors are required to use secure and/or encrypted methods authorized by Xtend before sending confidential information to parties outside of the organization.

Ensure Authorization
Employees and contractors are required to have reasonable assurance that the recipient of confidential information is authorized to receive the sensitive information prior to sending.
Do Not Disclose Unless Authorized
Employees and contractors are allowed to disclose sensitive information only when authorized to do so. Employees and contractors should never disclose information if they have any doubt they have authority to do so.

Store Sensitive Information Securely
Employees and contractors are forbidden to store sensitive information insecurely, either in hardcopy form or electronically where accessible to unauthorized personnel. In addition, users are not allowed to store sensitive information to their local machine or mobile device.

Data Leakage
Employees and contractors are forbidden to transfer sensitive information to mobile storage devices (such as to CDs or DVDs, or USB Flash Drives), unless such transfer is permitted by the organization to do so.

Notify When Suspected Security Incident Occurs
Employees and contractors are required to notify the organization when a breach of sensitive data is known or suspected.

Destroy Sensitive Information Securely
Sensitive information, especially in hardcopy form, should be destroyed when not used. Sensitive information in hardcopy form must be shredded in an authorized bin.

Passphrases and Passwords
Employees and contractors are responsible for safeguarding their passphrases and passwords for access to Xtend Computer Resources. Individual passphrases and passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passphrases and passwords. No Employees and contractors may access Computer Resources with another employee’s or contractor’s password or account, except in a support role with accompanying documentation. Employees and contractors should follow any passphrase or password guidelines as established by Xtend.

Passphrases and passwords do not imply privacy. Xtend has global passwords that permit access to all material stored on its Computer Resources regardless of whether that material has been encoded with a particular employee’s or contractor’s passphrase or password.

Building Security Requirements
The following are the core rules with respect to the security of the building:

Sign in for Access
All visitors except young children are required to sign in and have badges for entrance into the secure areas of any facility owned or leased by Xtend. Young children must be escorted at all times by a Xtend employee. Visitors are never to be left unattended.

Secure Access
All facilities leased by Xtend are considered secure requiring a badge for access. Visitors must be escorted, except for the front desk and training areas in the 28th street ground level.
**Badge Colors and Access**
Badges must be visible at all times. It will be the employee’s responsibility to advise the corporate officers immediately of any lost badge. Employees who lose their badges will be issued one free replacement; subsequent replacements will be $10.00 each. Color of badges determines the level of access.

**Visitor Access**
If Xtend employees encounter a visitor in a secure area without a badge, it is the responsibility of employees to politely inquire into the purpose of the visitor’s visit. If amenable, the visitor should be escorted back to the front desk and be provided both a badge and an escort to their location.

<table>
<thead>
<tr>
<th>Red Badge</th>
<th>Yellow Badge</th>
<th>Blue Badge</th>
<th>Green Badge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visitor</td>
<td>Approved Guests</td>
<td>Long Term Contractors</td>
<td>Employees</td>
</tr>
<tr>
<td>Visitors must sign in and be escorted in all facilities at all times in secure areas</td>
<td>Must sign in, but do not require an escort through the facilities</td>
<td>Do not need to sign in or be escorted.</td>
<td>Do not need to sign in or be escorted.</td>
</tr>
</tbody>
</table>

**Keyfobs**
Office access is restricted and must be granted through either electronic verification of the employee's key-fob or personally by an employee. A loss of a keyfob must be reported immediately. For visitors, the corporate officers may require this visitor or contractor to provide car keys or other valuables as a surety for the return of the keyfob.

**Access by Landlord(s) and Security Contractor**
Special access privileges are granted to both the building landlord(s) and contracted security companies. These are outside of the key-fob policies so that these individuals can access the building in case of emergencies involving the physical building systems (such as a security alarm or dealing with an HVAC problem during off hours). Both the landlord and the security companies have keys to the building that will allow them to access all floors of both buildings, including restricted areas. However, in off-hours a Xtend employee must be present to disable the alarm.

**Building Alarm Access**
Employees who are not granted privileges to arm and disarm the building based on the reasons outlined above, can be in the building only during normal business hours or after an authorized person has disarmed and opened the building. All contractor employees will not be granted any access to the building and must ring the doorbell to gain access even during normal working hours.

Employees will be restricted as to which alarm panel they can use to disarm and arm the alarm system, according to where their primary workstation is located and/or where the job duties are being performed.
**False Alarms**
Employees who set off the alarm falsely will receive one warning before being potentially fined to cover any expenses charged to Xtend for these violations (such as the Police Department costs).

**End of Day Protocols**
The last employee to leave a secure area must have alarm privileges. It is the responsibility of this employee to activate the alarm at the end of the night. This is true for all floors. This employee is responsible to ensure no other employees remain in the secure area. This employee must also check to see that no coffee pots remain on and all lights are turned off.

At least two employees shall complete the End of Day Protocols.

**WARNING**
Any employee failing to activate the security system when they are the last to leave the building will be subject to corrective action ranging from suspension up to and including termination.

**Employee Separation**
Employees who are terminated due to corrective action must be escorted immediately from the building.

**Security Cameras**
Xtend utilizes cameras to aid in visitor verification, key area monitoring, and vendor deliveries. Cameras are located at all major entrances and thoroughfares.

**Social Engineering Avoidance**
Xtend employees and contractors should always be aware that criminals have interest in using social engineering techniques to gain access to sensitive information. The awareness and integrity of an employee is the best line of defense for protecting sensitive information.

Employees and contractors must be aware of the types of social engineering attacks. These may include, but not be limited to telephone, email, letter, personal contact or other electronic means (instant messenger, text messaging, etc.). In addition, social engineering may include any attempt by any individual (including internal employees or in-person contact) to gain information via pressure techniques - i.e. social pressure, social encouragement or simply being tricked or deceived. Employees should always avoid clicking on links or opening attachments from unknown or suspicious sources. If any employee or contractor encounters a social engineering attempt, the employee should contact the Security Incident Response team. For in-person social engineering attempts, the employee or contractor should contact a member of the Security Incident Response team or the employee’s immediate manager.
What is “Cybersecurity?”

Legally, cybersecurity refers to the regulatory laws governing computer (or information) security. These laws cover compliance requirements, penalties for non-compliance, and victim remedies.

In addition, victims may have a right to sue due to negligence in handing sensitive information, unfair or deceptive practices, breach of contract, or privacy violations.

<table>
<thead>
<tr>
<th>TOP 10 THINGS TO KNOW ABOUT SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ALWAYS USE A STRONG PASSPHRASE:</strong> Passphrases are stronger than passwords. I want to go to Jupiter! is better and easier to remember than Jup1t3r!. A best practice is for network passwords to be at least 12 characters. Passphrases and passwords must include two of the following three: special character, capital, or number. Spaces are considered special characters and are useful!</td>
</tr>
<tr>
<td><strong>NEVER GIVE OUT YOUR PASSPHRASE:</strong> No employee should give out his or her password to anyone. If anyone ever asks for your password credentials over the phone or email, assume you are being social engineered.</td>
</tr>
<tr>
<td><strong>USE SEPARATE PASSPHRASES FOR SEPARATE SYSTEMS:</strong> Never duplicate your password for the various systems.</td>
</tr>
<tr>
<td><strong>NEVER SEND SENSITIVE INFORMATION INSECURELY:</strong> Personally Identifiable Financial Information (PIFI) is data that includes a persons’ name plus additional sensitive information such as the person’s social security number, account number, or credit card number. This information can be used to compromise the persons’ identity or steal their funds. Any email that must contain PIFI going outside our network must be encrypted through approved technology.</td>
</tr>
<tr>
<td><strong>SHRED SENSITIVE INFORMATION:</strong> Documents containing PIFI should never be thrown in the trash. Xtend has several shred bins located throughout the organization. Ripping documents up is not sufficient. If there is any doubt about the sensitivity of the information in a document, use the shred bins. Documents with sensitive data should not be left unattended and should be locked in desk drawers when not in use.</td>
</tr>
<tr>
<td><strong>KNOW THE BADGE RULES:</strong> There are three simple rules to follow regarding badges. Red badge visitors must be escorted when in a secure area. Individuals without badges must sign in and obtain a badge before entering a secure area. Never allow an unescorted visitor into a secure area. See the Building Security Policy for more information.</td>
</tr>
<tr>
<td><strong>DON’T DOWNLOAD UNAUTHORIZED SOFTWARE:</strong> Software downloaded from an un-trusted source may compromise your system or the entire network. If you need software installed on your system, fill out the appropriate form.</td>
</tr>
<tr>
<td><strong>AVOID OPENING ATTACHMENTS OR CLICKING LINKS FROM UNKNOWN SOURCES:</strong> Because we handle sensitive information on a daily basis, our employees will regularly be attacked by individuals looking to steal this data. Be very cautious if you receive an unexpected link or attachment in your email.</td>
</tr>
<tr>
<td><strong>IF YOU BELIEVE YOU HAVE BEEN COMPROMISED, CHANGE YOUR PASSPHRASE IMMEDIATELY:</strong> Everyone has the potential to be the victim of a social engineering attack. If you believe you have been compromised, the first thing to do is change your password. Immediately changing your password can prevent an attack.</td>
</tr>
<tr>
<td><strong>REPORT ANYTHING SUSPICIOUS TO COMPANY OFFICERS:</strong> Anything that might be suspicious should be reported to the company officers.</td>
</tr>
</tbody>
</table>
3. INFORMATION SECURITY POLICY AND PROGRAM

Policy Purpose and Overview
The Guidelines for Safeguarding Member Information (Guidelines) set forth standards pursuant to sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. These Guidelines provide guidance standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of member information. These Guidelines also address standards with respect to the proper disposal of consumer information pursuant to sections 621(b) and 628 of the Fair Credit Reporting Act (15 U.S.C. 1681s(b) and 1681w).

This Information Security Policy and Program is designed to:

• ensure the security and confidentiality of member information;

• protect against any anticipated threats or hazards to the security or integrity of such information;

• protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member; and

• ensure the proper disposal of member information and consumer information.

The Xtend Information Security Program is designed to provide clear guidance to all staff on the minimum standards of data protection. This Program also provides guidance on the regulatory and contractual obligations Xtend must fulfill to continue in business. Xtend aspires to the best possible security of sensitive information within the bounds of commercial reasonableness. Xtend enforces this program through technical controls and audits.

Data Classification
Xtend relies on just two categories of data classification: data is either sensitive or not sensitive. Sensitive data must be protected in accordance with this Information Security Program and all policies of Xtend. Data that is not sensitive does not require security controls, although employees are cautioned to use information in accordance with the Employee Handbook and Acceptable Use.

Examples of Sensitive Information
Examples of sensitive information include but are not limited to: the fact that an individual is the customer of a particular financial institution; consumer’s name, address, social security number, credit card number, or account number; any information a consumer provides on an application; information from a “cookie” obtained in using a website; and information on a consumer report obtained by a financial institution (NOTE: Such information may also be covered by the Fair Credit Reporting Act).
Program Implementation
This Policy and Program is implemented by the Xtend Board of Directors. Executive management is responsible for oversight. Vendors must agree to meet the requirements of the law if they have access to sensitive member information.

Risk Assessment
The program will have a risk assessment performed on no less than an annual basis and directed against the foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems.

This Program risk assessment will assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of member information.

The Program risk assessment will assess the sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.

Manage and Control Risk
Xtend will design the Information Security Program to control identified risks and implement commercially reasonable security controls, including: access controls on information systems with sensitive data; restrictions on physical access to information systems; reasonable efforts to provide encryption of sensitive information; procedures designed to ensure security during and after system modifications; as appropriate, dual controls procedures, segregation of duties, and employee background checks for employees; monitoring systems and procedures to detect actual and attempted attacks on or intrusions into information systems; response programs that specify actions to be taken when Xtend suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies; review whether member information disposed of properly; and measures to protect against destruction, loss, or damage of member information due to potential environmental hazards, such as fire and water damage or technical failures.

Staff is trained to understand and implement this program. Controls will be tested both internally and by external parties. As part of this program, appropriate measures will be taken to properly dispose of member information.

Security Breach
Defined as when Xtend is aware or suspects that a breach of sensitive data has taken place. A breach is whenever sensitive data has been exposed to an unauthorized party.

A breach of member data may result in a forensic investigation with the involvement of law enforcement and regulatory authorities.

Incident Response Protocol
The purpose of this policy is to provide guidelines for responding to a service or security issue broadly impacting one or more client credit unions. The basic process flowchart is on the following page.
# INCIDENT RESPONSE PROTOCOL

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>REPORT</strong></td>
<td>Upon report of a potential vulnerability, the Xtend Team becomes involved, and individual members are assigned priorities, such as client contact, research, and communication with executive management.</td>
</tr>
<tr>
<td><strong>RESEARCH</strong></td>
<td>Xtend performs research on the scope of the issue. The primary focus is to determine whether the issue is global, and therefore warrants removing a system from all client access until the problems can be resolved.</td>
</tr>
<tr>
<td><strong>REVIEW</strong></td>
<td>Xtend executive management is provided evidence, or lack thereof, of the scope of the security threat.</td>
</tr>
<tr>
<td><strong>NOTICE</strong></td>
<td>Crisis communications are set up, when warranted. Depending on the scope of the issue, this may include a notice to all clients, or communications with just the affected credit unions.</td>
</tr>
<tr>
<td><strong>ETA</strong></td>
<td>When warranted, communications are sent to clients including uptime and downtime estimates for service interruptions.</td>
</tr>
<tr>
<td><strong>PATCH</strong></td>
<td>If patches are required, these follow the same control testing process as other patches in the environment.</td>
</tr>
</tbody>
</table>
Roles: Incident Response Team (IRT)
An IRT may be called together at any time Xtend is aware of a potentially serious breach of security. The IRT will coordinate resources to investigate and resolve the problem. Corporate officers will make the determination to involve counsel, law enforcement, regulatory agencies, and the communication to clients and vendors. Corporate officers may determine that outside expertise is necessary to effectively deal with the incident. In such cases, any of these positions may retain such help as necessary to deal with the immediate threat. All such activities must be documented.

Credit Union System Vulnerability
In some cases, Xtend might need to take the serious step of disabling access to a credit union system due to a security breach. This process will not be invoked until there has been a proper review of the incident.

CREDIT UNION PROCEDURES
Xtend strongly recommends that the credit unions create internal procedures to handle this situation and educate staff on reporting responsibilities and escalation procedures.
Examination Protocol

This document is intended to establish general guidelines for any agency, individual or audit firm performing an audit or regulatory exam at Xtend. This protocol is intended to streamline the audit process, ensure that all appropriate individuals are involved from the outset of the audit/review, reduce the overall time associated with the process, and assure that any audit findings are based on correct information.

If any procedures outlined result in significant burden on behalf of any department being reviewed or on the external audit firm or agency, Xtend will work with the department or auditor to modify this protocol as necessary.

Scheduling
Requests for audits should be made in advance to Xtend. Advance arrangements ensure that the appropriate individuals are available to assist the examiners, relevant records are located and available, any interviews are scheduled to provide minimum disruption of departmental activities, and required facilities and services are available.

Entrance Conference
The designated representative will schedule an entrance conference with the external auditing team. The entrance conference may be held by a teleconference if all affected parties agree. All parties must be aware that the meeting and subsequent discussion is intended as an entrance conference. During the entrance conference, Xtend requests that the external auditors provide the following information: scope of audit; timing of the audit, including estimated start and completion dates, deliverables and reports; requesting agency or individual as applicable, external audit team personnel, including designation of an audit lead; contact information and work schedules of onsite visits; and processes to allow the Xtend audit team the opportunity to review and comment on the deliverables and reports, including any draft findings and the final audit report.

As appropriate, weekly status calls and/or meetings may be requested and scheduled. Written track will be kept of all follow-up items, and these items will be reviewed at the next meeting.

Changes to Schedule
Xtend shall be informed as soon as possible of any known changes in audit timelines, deadlines or changes in scope, external audit team personnel, contact information or other pertinent or important information.

Information Requests
All anticipated material and interview requests should be made at least 30 days prior to the audit start date. Information in these requests will be prepared and provided to the external auditors by the audit start date. All requests for information must be in writing, including the requested return date of the information. If the request for information is considered informal, the request must be followed
up in writing. The Internal Auditor will inform the external auditors if the audit requests cannot be reasonably accommodated in the requested time and provide an estimated deliverable date.

**On-Site Requests for Interviews**
Information requests made on-site may take more than one day, depending upon the information requested. Xtend will make every reasonable effort to provide information in an efficient manner to external auditors. Xtend requests a minimum of 48 hours to respond to and provide large data and information files to on-site external auditors.

**Findings**
Potential findings shall be communicated to Xtend as soon as possible. Xtend shall have a minimum of thirty days to prepare and offer rebuttal to any potential findings. If any external auditor experiences a delay, lack of responsiveness, or an item of concern from Xtend personnel, the external auditor shall inform Xtend immediately. Xtend shall make every reasonable effort to assist in the resolution of the problem.

**Exit Conference**
Upon notification from the auditors that the onsite audit has been completed, Xtend will schedule an exit conference. The exit conference may be held via telephone, teleconference or in person, as long as mutually agreed upon by all affected parties. The external auditors will not introduce any new findings or information at the exit conference. As long as proper protocol is followed, all issues, findings, information, and concerns will have been provided and discussed prior to the exit interview.

The external auditors shall provide written documentation of potential findings to Xtend. A mutually agreed upon response time shall be discussed during the exit interview or subsequent communication between auditors and Xtend.
4. ACCEPTABLE USE POLICY

Policy Purpose and Overview
Xtend relies on its computer network to conduct its business. To ensure that its computer resources are used properly by its employees, independent contractors, agents and other computer users, Xtend has created this Acceptable Use Policy. The rules and obligations described in this Policy apply to all users of Xtend’ technology, wherever they may be located.

Technology that is the property of Xtend may only be used for legitimate business purposes. Users are permitted access to the technology to assist them in the performance of their jobs.

It is every employee’s duty to use Xtend’ technology responsibly, professionally, ethically, and lawfully. In the use of technology, Users must observe and comply with all other policies and guidelines of the company.

Definitions and Prohibited Uses

Unlawful or Inappropriate Material
Material that is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by email or other form of electronic communications or displayed on or stored in Xtend’ computers. Users encountering or receiving this kind of material should immediately report the incident to their supervisor(s).

Employees are prohibited from using Xtend Internet access or a Xtend provided device to view sites considered to be sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate to view.

Other Prohibited Uses
Without prior written permission from a Corporate Officer, Xtend’ Computer Resources may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, viruses or malware, political material, chain emails, or any other unauthorized use.

Misuse of Software
Without either prior authorization or as part of a job function, Users may not do any of the following with software provided by Xtend: copy software for use on their home computers; provide copies of software to any independent contractors or clients of Xtend or any third person; install software on any of Xtend’ workstations; modify, revise, transform, recast, or adapt any software; or reverse-engineer, disassemble, or de-compile any software. In their use of technology, Users must comply with all software licenses; copyrights; and all other state, federal and international laws governing intellectual property and online activities.

Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisors.

Unsupported Technology
Xtend must strike a balance between innovation, effectiveness, and security when Users wish to install unsupported software or hardware which is not issued by Xtend. Unregulated installation of
software and hardware may result in confidential data leakage, weak security, unavailability in a disruption, access control, and lack of “liquidity” of tools, where the vendor cannot be changed easily if the vendor fails to perform. However, in the interest of innovation and effectiveness, there is a process where tools can be approved for use by the organization.

**No Expectation of Privacy**
Technology provided to Users by Xtend are to assist Users in performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive on any technology, or with respect to calls and voice recordings made via the telephones and related voice technology owned and operated by Xtend. Technology owned by Xtend may be used only for business purposes.

**Accessing the Files of Another User**
Users may not alter or copy a file belonging to another user without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to “snoop” or pry into the affairs of other users by unnecessarily reviewing their files and email.

**Accessing other Resources**
A User’s ability to connect to other technological Resources through the network does not imply a right to connect to those Resources or to make use of those Resources unless specifically authorized by the operators of those systems.

**No Local Administrator Rights**
Users should not expect to have Local Administrator rights on their machines unless an exception is granted by the Executive Team. Exceptions may be granted upon a showing of business need and completion of the proper form.

**Unauthorized Technology or Software**
Users are responsible and may be disciplined for any security breaches related to the use of unauthorized technology or software.

**Duty to Secure**
Each User is responsible for ensuring that use of technology, as well as outside computers and networks, such as the Internet, does not compromise the security of Xtend. This duty includes taking reasonable precautions to prevent intruders from accessing the company’s network without authorization, preventing introduction and spread of malware, and the use of other reasonable means to protect sensitive information.

Users must take reasonable steps to ensure sensitive information is maintained and transmitted securely. Users must not disclose sensitive information unless authorized by job description or by an officer of Xtend.

Consult the Cybersecurity Policy for additional information on the requirements for protecting sensitive information.
Electronic Communications
Examples of electronic communications include but are not limited to: email; messaging (both text and instant); and social media. A User should never consider electronic communications to be either private or secure unless encrypted with Xtend approved encryption software. Note that electronic communications may be stored indefinitely on any number of computers, including that of the recipient and any individuals the recipient has forwarded the electronic communications onto.

Encryption of Sensitive Information
Users who send or receive sensitive information via electronic communications are required to use encryption when this information is sent out beyond the Xtend network borders (such as external email recipients).

No Expectation of Privacy on the Internet
Users who post Information on the Internet should not consider the data to be private or secure, even when a User is employing a private feature of an electronic communications site. Do not rely on the privacy controls of the provider to keep communications confidential.

Logos and Marks
Do not use without authorization the Xtend name, names of partners, clients or their logos that would infringe on the intellectual property rights of the owner. If a User has a personal blog where advice or opinion is offered on work-related matters, add a disclaimer to the homepage that states the comments are personal opinions and do not necessarily reflect the opinion of Xtend or any of its partners or affiliations.

WARNING
Xtend does not audit the personal electronic communications of Users with respect to non-work-related matters. However, should a personal electronic communication be brought to the attention of Xtend which adversely affects the reputation of Xtend or involves the unauthorized dissemination of sensitive information, this data may be used to discipline the User or terminate employment.

Remote Desktop Support
From Third Parties
Users may require a third party to provide remote desktop support. The following are the rules for obtaining remote desktop support from third parties.

Permission Required
Users participating in remote access sessions with third parties must first obtain permission from their manager or supervisor.

Physical Attendance Required
A User participating must not leave the PC at any time, in order to observe the actions of the third party.
**Software Installation Requirements**  
Installation of software in a remote access session is governed by the software installation rules of this policy.

Users may need to support clients through remote desktop support. Users must adhere to all policies and procedures of CU*Answers while engaged in remote session support of a client.

**Mobile/Remote Computing and Access**  
Xtend recognizes that some Users may require mobile or remote access to technology. This access may include but is not limited to VPN access, a Xtend provided laptop or tablet, or access through a personal device. In addition to the other acceptable use rules encompassed in this policy, employees are required to follow these additional policy rules:

**Approval Required**  
Mobile or remote access to any Computer Resource requires approval by the departmental supervisor and the CEO. Xtend reserves the right to deny remote access at any time if the device does not meet minimum secure access requirements. An employee who has not completed the 90-day probationary period is not allowed remote access to Xtend unless an exception is made by a corporate officer.

**Minimum Security Standards**  
Any device used to connect remotely to Xtend must be secured by a password. Remote access requires the device to maintain a secure, encrypted connection between Xtend and the local machine. Only approved mobile device management software may be installed on the user’s PC for the purpose of updating the device with operating system updates and/or syncing of corporate data.

**No Local Save of Sensitive Information**  
Employees are expressly forbidden to save sensitive information to any local machine that has mobile or remote access to Xtend.

**Consent to Remote Wipe**  
All Users must consent to have their mobile access device, whether personal or Xtend issued, remotely wiped in the case of termination of employment, loss of the device, or suspicion of a security breach. Xtend is not responsible for any loss of personal information which may be stored on the device.

**Lost or Stolen Device**  
If the local machine used to connect remotely to Xtend is lost or stolen, employees are required to immediately notify a security officer or a supervisor.

**VPN**  
The use of VPN to connect to Xtend is strictly prohibited except for approved devices. Users are never allowed to connect using VPN on machines that are accessible to the general public. Xtend has the right to terminate any VPN connection at any time if the security of the connection is in question. VPN connections to Xtend are strictly limited for business purposes only. No VPN connection may be maintained for longer than five minutes unattended without security measures such as screen-locking employed. Users may never allow any unauthorized individual to access Xtend through a VPN connection.
Endpoint Security

As part of Xtend ongoing Data Leakage Control program, all devices shall be restricted to Read Only access for attached USB mass storage devices and optical media drives including but not limited to CD-ROM/CD-RW drives and DVD-ROM/DVD-RW drives. Data execute, write, and modify access is restricted. Where exceptions are made, member data must not be copied to, stored on, or moved by unencrypted USB mass storage or optical media. In order to have an exception, a form must be filled out and permission granted.
5. LARGE SCALE ABSENCE POLICY

Large Scale Absence Program
A large-scale absence, for purposes of this document, is defined by Xtend as missing 50% or more of the employee population for a period of up to 2 consecutive weeks. The determination Xtend is experiencing a large-scale absence event will happen at the CEO level.

Methodology
Team leaders assessed specific needs and concerns faced in a large-scale absence event for their area(s) within the company. These needs and concerns, the response or reaction to those concerns, and any preventative measures that can be taken have been used in the development of this planning document.

Client Serving
Delays in servicing our clients should be expected. However, Xtend will communicate delays to clients appropriately by sending out a scripted message using our Alert procedures.

Coverage of All Shifts
Management will ensure all necessary shifts are covered across all areas of the company. Employees and managers who have the capability to work from home may be encouraged to do so, if the situation allows.

Prioritizing Daily and Pending Duties
Time sensitive items must be considered. For example, if the timeframe is end of month, team members must be diverted across departments to complete important tasks. Management shall make decisions on readjusting the priority list and delay of non-critical project travel.

Managing Project Timelines
Management will adjust these timelines and workloads.

Delivery
Handling the Essential Duties
Essential duties will be assigned by management as necessary. If possible, management will adjust timelines and workloads by re-prioritizing duties.

Operations
Management shall adjust schedules of remaining team members to cover all shifts and run with reduced staff per shift. Managers will provide additional coverage as needed.

Cross-Departmental Coverage
Employees from other teams will be drawn upon to cover gaps in processing shifts in the event of a serious shortage in Operations staff.
**Travel During Event**
The travel expectations during an event will be decided upon by Xtend Corporate Officers and communicated to the employees through ORD. Depending on the circumstances surrounding the event, any decision could be made up to and including the suspension of all travel.

**Additional Pandemic Policies**
If the absence is due to a pandemic disease, Xtend shall develop protocols for cleaning workstations, social distancing, and remote work options.

Staff interactions during an event will be decided upon by Xtend Corporate Officers and communicated to the employees through ORD. Depending on the circumstances surrounding the event, decisions will be made regarding:

- Severely discouraging or disallowing large assemblies of employees (on or off work premises);
- Closing all meeting rooms; limiting all staff interactions as much as possible; encourage or force employees to work at home or at other CU*Answers offices; and/or
- Offering masks and setting up for cleaning stations around the office.
6. RECORDS POLICY AND LITIGATION HOLD

Scope and Definitions
Records and information management (RIM) is the systematic control of all records, regardless of media, from the point of their creation or receipt, through their processing, distribution, organization, storage, and retrieval, all the way to their final disposition. Information flows through the organization in the form of paper and electronic records including but not limited to word processing documents, spreadsheets, e-mail, graphical images, and voice or data transmissions. Information can be stored on a variety of storage media, such as microfilm, microfiche, diskette, optical disk, CD-ROM, videotape, and paper.

Unless mandated by law, regulation, contractual obligations, or as the result of a litigation hold, there is no legal duty to preserve information generated in the course of business.

Principles
This policy details the requirements and responsibilities to initiate a well-defined RIM program. The RIM program applies to those departments that require a long-term records-retention, -storage, and -disposition program. Absent specific, written provision to the contrary, it is presumed that the RIM program applies to all departments within Xtend.

Internal Records Only
This policy applies to Xtend records and information. Records and information managed for clients is governed by the clients’ own RIM policies and the agreements between the clients and Xtend.

Preserve Only Records of Value
Ensure only essential records of continuing value are preserved. Records should be retained in the active office areas as long as they serve the immediate administrative, legal, or fiscal purpose for which they were created.

Establish Safeguards
Establish safeguards against the illegal removal, loss, or destruction of records. Records either should be disposed of in accordance with an approved records-retention schedule or transferred to the records-retention center until the prescribed retention period has expired.

Responsibility of Owner/Creator
Management of records is the responsibility of the owner or creator, of the record. Xtend will ensure that one or more Records Managers will be designated for each department to assist in the implementation of the RIM program. The department director or the director’s designated representative should remain in periodic contact with the Records Manager to discuss initiating the records-management program or reviewing an existing records-management program to handle records properly from their creation through their destruction. Departments can be provided guidance on how records should be organized and stored to ensure timely and efficient retrieval.
Retention Schedule
The records-retention schedule is the key tool for departments to use to manage their records effectively. Information is a valuable asset; however, if records that contain information cannot be retrieved efficiently or are retained beyond their legal, regulatory, or administrative retention period, they lose their value and may impose a liability to Xtend.

Litigation Hold
If a litigation hold is appropriate, the hold notice should be issued as soon as practical. The notice should identify the data that are subject to the litigation hold and advise all employees not to delete, overwrite, or otherwise alter or destroy any records (paper or electronic) that may contain information that is reasonably related to the identified subject matter. The notice should also make clear that this obligation applies to records that currently exist or are created in the future. The litigation hold notice should include directions to all Xtend employees to advise if that employee has any paper or electronic records related to the litigation hold in his or her possession so that the information can be collected in a timely manner. The notice should also describe all the types of media where records may be stored—e.g., laptops and all other portable devices, such as cell phones, home computers, and voice mail. The notice should advise that all data, even data on back-up tapes, should not be overwritten or rotated until further notice.
7. VEHICLE POLICY

Definitions
The following definitions apply to this policy:

Company Vehicles
"Company Vehicles," for purposes of this policy, pertain to all vehicles in the pool available to all eligible employees travelling on Company Business and to any vehicles leased by Xtend for use by a specified individual.

Rental Vehicles
“Rental Vehicles,” for the purpose of this policy, pertain to all vehicles rented by Xtend to eligible employees travelling on Company Business.

Company Business
"Company Business" for the purpose of this policy, pertains to any activity the employee engages in under the direction of, or on behalf of, Xtend. This does not pertain to regular commuting to and from work.

Driving Related Position
A "Driving-Related Position" for the purpose of this policy, pertains to a position that has been determined by Xtend to require driving of either the employee’s personal vehicle or a Company Vehicle for Company Business.

Scope
The policy applies to all use of Company Vehicles, rental vehicles and the use of personal vehicles for Company Business.

Eligible Drivers
Every employee who operates a Company Vehicle, a rental vehicle, or operates a personal vehicle on Company Business must have a valid and current Driver’s license. Current auto insurance is required for any use of a personal vehicle for Company Business. Drivers are required to provide proof of insurance and a state-issued driver’s license on no less than an annual basis.

Motor Vehicle Records are obtained:

- Prior to employment on all candidates for Driving-Related Positions; and

- Periodically during employment as deemed appropriate by Xtend on all employees performing Driving-Related Positions. Consent to such inquiries is a condition of employment in a Driving-Related Position. An unacceptable driving record will result in disqualification for a Driving-Related Position.

Any employee in a Driving-Related Position who has a driver’s license revoked or suspended will immediately notify the ORD Team within 24 hours of the revocation or suspension and immediately
discontinue use of Company Vehicles or driving on Company Business. Failure to follow this procedure may result in disciplinary action up to and including termination.

**Driving Record Criteria**

**Good Driving Records**
Employees in Driving-Related Positions are expected to maintain good driving records, and follow the reporting criteria above when incidents that affect their record occur. If a pattern of unsafe or irresponsible driving is detected, a decision may be made to suspend or revoke the driving privileges of the employee at the discretion of the company officers.

Criteria of an unacceptable record may include, but are not limited to, three or more moving violations in a year.

**Violations**
Violations include:

- Any ticket, citation, or other law enforcement determination relating to these;

- Three or more chargeable accidents within a year where chargeable means the driver is determined to be the primary cause of the accident through speeding, inattention, etc. (factors such as weather or mechanical problems will be taken into consideration);

- Any combination of accidents and/or moving violations; or

- Any driving violation or infraction that results in the employee being ineligible for insurance coverage under the policy or policies applicable to Company Vehicles.

**Acceptable Use of Vehicles**
Company Vehicles are to be driven by authorized employees only and limited to use for Company Business except as otherwise authorized in writing by Xtend.

With respect to any driving for Company Business, travel should generally be limited to that necessary for the Company Business, and not include significant deviations from route or schedule for personal matters. This provision does not preclude incidental, occasional personal stops provided they do not interfere with the employee's performance of his or her duties.

**Driver Safety Rules**
Any violation of the safety rules below while operating a Company Vehicle, rental vehicle or a personal vehicle for Company Business will be grounds for disciplinary action up to and including termination:

- The use of a mobile device for written communication, including but not limited to texting and emailing, is strictly prohibited. The law in Michigan defines that a person shall not read, manually type, or send a text message on a wireless 2-way communication device that is located in the person’s hand or in the person’s lap, including a wireless telephone used in a cellular telephone service or personal communication service, while operating a motor vehicle that is moving on a highway or street.
• Cell phone use for verbal communication while driving should be kept to a minimum. Drivers need to be aware when use of the cell phone is creating a distraction from safe driving and adjust their usage accordingly, including pulling off the road to continue and/or finish the conversation if needed. Whenever possible, drivers should complete calls while the vehicle is parked and/or use the phone in a “hands free” mode via a headset or speaker.

• All drivers and passengers operating or riding in a Company Vehicle or rental vehicle must wear seatbelts, even if air bags are available.

• Drivers are responsible for the security of Company Vehicles and rental vehicles assigned to them, ensuring keys are removed and doors are locked when the vehicle is unattended. Employees may often be travelling with company or client property in the vehicles; proper precautions must be taken to ensure the safety and care of this property.

• All laws must be obeyed.

**Maintenance of Vehicles**

When the Company Vehicles are not in use they are to be left in Xtend’s Main office parking lot. The mileage log booklets must be completed by the employee after/during each use and is to be kept in the glove box of each Company Vehicle.

The Company Vehicle should always be returned clean and with a full tank of gas when possible; please notify the Facilities Management if the tank is half full or less when you return to the office.

Smoking in Company Vehicles is strictly prohibited.

Each Company Vehicle shall be regularly maintained by the facilities technician. Any necessary maintenance or repairs detected by the employee while operating the vehicle shall be reported to Facilities immediately.
8. VENDOR MANAGEMENT POLICY

Vendor Management Program
The Vendor Management program is to help mitigate and manage that risk. Risks may include:

- Reputational risk through the misuse of sensitive or confidential data;
- Transaction risks such as fraudulent activity;
- Strategic Risk relative to the dependency of service provided; and
- Compliance risk primarily in the area of GLBA.

A regular review of these vendors and their continued ability to provide services in a safe and sound manner is an essential process in mitigating these risks.

Oversight
Vendor oversight through this program is the responsibility of the sponsoring team and the Corporate Officers. Not all vendors are subject to this level of risk review as determined and documented during the risk assessment process.

Vendor Risk Oversight
TIER I
Tier I vendors pose the highest degree of risk and require the largest degree of ongoing due diligence. Vendors that fall under this tier generally meet one or more of the following criteria:

- Have access to, transmit, or store a large amount of non-public member data;
- Would have a significant impact on income and expense statement in the event of its dissolution or contract termination;
- Would be difficult to replace in a reasonable period of time while seriously disrupting service;
- Have high level access to IT infrastructure behind the firewalls where corporate secrets and member information reside; and/or
- Have access to the facilities in an unescorted manner and in doing so may also have access to member data.

TIER II
Public Companies that provide a service technical in nature that may house member data. A Tier II company may also have a significant impact on income and expense statements.
TIER III
Tier III vendors generally will have some degree of access to non-public member data, they are not as difficult to replace quickly, and have no access to the credit union's network or physical locations. Typical vendors that fall into this category would be private mortgage and credit life and disability providers.

TIER IV
These vendors would consist of public companies that could be viewed as vital to the community infrastructure. If a company of this type were to fail it would have regional catastrophic effects. Companies that fall into this category generally are the public utilities. These companies are considered critical, however the failure of these types of companies is highly unlikely as they are vital for the community or region to survive. Contingency and disaster recovery plans or more important in this case to manage the impact of their failure vs. the management of the vendor relationship. Examples of these type of companies would include DTE Energy or Consumers Energy.

TIER V
Companies that fall into this tier may come into contact with member data or have physical access to the facility. Generally, these companies would have very little direct access to information, can be replaced very quickly, and would have little if any impact on the ongoing business operations of the credit union if they fail.

Evaluation Process
Based upon categorization Xtend will require some or all of the following events tracked:

- News feeds.
- Annual or audited financial statements (or quarterly financials if it is an owned CUSO).
- Publicly available control audit.
- Insurance/bond.
- Internal network infrastructure audit or penetration test.
- Disaster recovery/business resumption policies and annual testing.

The following items are those that may be reviewed during the due diligence process:

- Review of financial statements, preferably audited statements.
- Review of insurance coverage.
- Contacting references and user groups.
- Determination if service provider performs background/reference checks on its new employees.
• Determination if third parties/contract employees would support the service provider in fulfilling its requirements.

• Conclude if the service provider uses third parties/contract employees. If so, what type of due diligence they perform on those third parties.

• Perform an onsite visit, if applicable.

• Review SSAE report if applicable.

• Determine service provider’s knowledge of GLBA, Regulation E, Privacy Act, Consumer Protection and Bank Secrecy Act.

• Determine how long the vendor has been in business.

• Conclude on the vendor’s experience and ability to provide service in question.

• Review disaster recovery/business resumption plan of vendor.

• Determine security precautions implemented, such as firewalls, encryption, authentication, etc.

• Compare market share in the given service area to competitors.

**Evaluation Reporting**

The assessment and analysis of all vendors will be completed, and then on an annual basis the vendors will be evaluated to determine if the criticality status has changed. Reports of vendor reviews, along with any specific recommendations, will be presented to the Board of Directors at least once a year.