

(Suggested Format) *

Information Handling Table

* Consult with general counsel prior to implementation of suggestions below

Information should be marked and handled according to its information classification. The four categories for information are:

- **Public Information** has been made public through authorized company channels. Information in this category includes marketing brochures, press releases, and the Annual Report.
- **Internal Information** is made available to employees and other authorized parties, such as information on the company intranet site or the employee directory.
- **Confidential Information** provides the company with a competitive advantage and disclosure could result in damage to us. Information in this category includes strategic business plans, financial forecasts, merger and acquisition information, and legal documents.
- **Customer Confidential Information** is a special type of confidential information about our customers, including Sensitive Customer Information (SCI) which is subject to special protections due to laws, contracts, or company policy.

Action	Internal, Confidential, and Customer Confidential Information
Creation	Handling practices around information creation help clearly convey the sensitivity of the information and limitations on distribution and disclosure.
Marking/Labeling (Physical)	<p>Loan Documentation: All loan files contain a borrower name, loan number and other sensitive customer information. All employees treat this information as SCI so there is no need to label each loan file or each document within the file to be further classified by type of information.</p> <p>Miscellaneous Documentation, including reports, memorandums, and policies: These documents should be marked directly on each page to show its information classification in the footer.</p> <p>It is not necessary to further label, mark or classified public information.</p>
Marking/Labeling (Electronic)	<p>The electronic repository in which the information resides is set up by departments on a need to know basis for users and no other employees have access. Shared network folders, systems, databases or applications are maintained with access limited to a need to know basis.</p> <p>Electronic files or emails sent to external parties should be labeled clearly with both the company name and, if SCI is included, then secure email procedures should be followed.</p>

Access Control	The creator should ensure that adequate access controls are in place to protect the information based on business need for access (need-to-know principle). This is accomplished through use of a shared drive within a department and user access only on a need to know basis.
Reproduction and Copying (Regardless of Form)	Unless a document states that reproduction is prohibited, copies of information may be distributed only to individuals with a business need to know the information.
Storage	Handling practices related to storage should provide reasonable protection of information, regardless of form, against unauthorized disclosure. Protection may include hardware, software, or other mechanisms that appropriately control access to Confidential or Customer Confidential information.
Storage in Physical Form	<p>Employees should ensure that unauthorized persons cannot view confidential information on monitors, bulletin boards, whiteboards, through windows, or in other ways.</p> <p>It is policy to secure locations by security access cards. In unsecured locations or unsecured areas within a secured location, employees should not leave Confidential or Customer Confidential information on desks unattended.</p> <p>Confidential information should be kept in desk drawers, filing cabinets, covered boxes, or other out-of-sight locations. Customer Confidential information should be kept locked in a secure area, room, desk filing cabinet, etc.</p> <p>Access controls are required for mass storage of private information (e.g., locked file room for storage of large amounts of Customer Confidential information).</p> <p>Cleaning crews should be bonded.</p>

<p>Storage in Electronic Form</p>	<p>Store only on secured company owned information systems.</p> <p>Sensitive customer information, including credit card numbers should be encrypted in storage on distributed platforms and portable media. Encryption should be done using company-approved encryption software or devices.</p> <p>Encrypted electronic storage of other company Confidential and Customer Confidential information is encouraged, but not required unless the system is Internet-accessible.</p> <p>Data stored on Internet-accessible systems should be encrypted using a company approved method.</p> <p>Data stored on portable computing devices and portable media, such as laptops, PDAs, floppies, CDs, smart phones, and USB drives, should be encrypted using a method approved by the company.</p>
<p>Sharing/Disclosure</p>	<p>Sharing and disclosure practices are primarily aimed at enforcing the need-to-know principle, ensuring that the sensitivity of the information is properly conveyed, and ensuring that third-party arrangements are properly addressed.</p>
<p>Conversation</p>	<p>Employees may discuss confidential information only with other company employees, contractors, temporary employees and other authorized third parties with a business need for the information.</p> <p>When using speakerphones, employees should ensure that unauthorized persons cannot overhear.</p> <p>Confidential information may be discussed only over approved cordless, wireless, or cellular phones or headsets.</p>
<p>Disclosure to Personnel; including Employees, Temporary Employees, and Contractors</p>	<p>Information may be shared only with company employees, contractors, temporary employees and other authorized third parties with a business need for the information.</p>

<p>Disclosure to Third-Party Business Partners (Clients and Service Providers)</p>	<p>Information may be disclosed only to third parties with a business need-to-know who have appropriate legal agreements executed.</p> <p>Company requirements regarding risk assessments and appropriate contract language for vendors and other third-party arrangements apply.</p> <p>Contracts with vendors are managed through a company Vendor Management Process. These procedures address Sensitive Customer Information and make specific contractual provision for the treatment of SCI.</p>
<p>Transmission</p>	<p>Controls around the transmission of confidential information ensure that such information receives a level of protection commensurate with its sensitivity and criticality as it traverses uncontrolled environments.</p>
<p>Electronic Transmission on Non-Company Networks</p>	<p>Information should be encrypted using company approved secure transmission facilities.</p> <p>Any vendor must be approved through the Vendor Management Process and meet all data security and firewall requirements to ensure the safety of all Customer Confidential information.</p>
<p>Electronic Transmission (Fax)</p>	<p>The sender should notify the recipient prior to transmission if recipient's fax machine or system is located in an unsecured area.</p> <p>The recipient should acknowledge receipt of the fax via phone or email.</p> <p>Incoming faxes should be made to fax machines in secured areas, or directly to the recipient's email inbox using approved company technology.</p> <p>Fax cover sheets should be used. The fax cover sheet should indicate if the fax contains sensitive customer information.</p>

<p>Mail/Delivery Using Non-Company Carriers such as USPS, UPS, FedEx, or Couriers</p>	<p>Sensitive Customer Information should be sent via secure UPS per company outlined procedures.</p> <p>Packages should be labeled "To Be Opened by Addressee Only."</p> <p>Packages should be left in a secure location for pickup by carrier (e.g., in carrier's drop box or other secure location).</p> <p>Information sent through overnight delivery companies is tracked to avoid lost or stolen files during transport.</p> <p>Refer to specific company requirements regarding shipping requirements of Sensitive Customer Information.</p>
<p>Mail/Delivery Using Company Carrier (Within a Single Location)</p>	<p>Sensitive Customer Information should be sent either in a double envelope with the internal envelope marked "Confidential" or "Customer Confidential" and the outer envelope marked "To Be Opened by Addressee Only" or in a single, sealed, tamper-evident envelope or package marked "Confidential" or "Customer Confidential."</p>
<p>Video Teleconferencing and Telephonic (Company and Non-Company Networks)</p>	<p>Should be conducted using company approved teleconferencing services.</p> <p>Employees should restrict the use of cellular phones to secure areas for discussing Sensitive Customer Information.</p> <p>Speakerphones may be used to discuss confidential information only in secure locations where conversation cannot be overheard by unauthorized individuals.</p>
<p>Retention, Disposition, and Destruction</p>	<p>Handling practices around the retention and disposal of classified information, or devices providing access to such information, help to ensure that business and legal requirements related to information retention are followed and that information released from the company's control for destruction is in an unusable/unreadable form.</p>
<p>Information Retention</p>	<p>All final active and canceled files should be housed in designated facilities.</p>
<p>Physical Document Disposal</p>	<p>All Sensitive Customer Information should be securely disposed of by shredding or putting into company-provided locked disposal bins.</p>

<p>Electronic Data Purging and Media Destruction</p>	<p>Purging, clearing, or destruction should reasonably prevent the reconstruction of information, regardless of medium (e.g. laptop, CD, PDA, workstation).</p> <p>Equipment should be processed according to the standards of the company for destruction or redeployment. Company approved tools should be used to remove/clean equipment of information upon transfer or return of the asset.</p> <p>Portable media, such as floppy disks/tapes, CDs, DVDs, flash drives, etc., should be physically destroyed, placed into an approved company-provided locked disposal bin for media devices, or disposed of using other company approved destruction methods.</p> <p>The Record Center is a secured site accessed through security card access with on site security system and guard.</p>
<p>Removing Information From Company Premises</p>	
<p>All forms of information</p>	<p>Controls around removing information from company premises (e.g., taking work home, on business trips, or to business partners' location) ensure that such information receives a level of protection commensurate with its sensitivity and criticality when removed from company facilities.</p>