

INFORMATION SECURITY PROGRAM

Program Objectives

The objectives of this Information Security Program (“Program”) are to create effective administrative, technical and physical safeguards in order to protect customer personal information. The Program will evaluate our electronic and physical methods of accessing, collecting, storing, using, transmitting, protecting and disposing of customer information.

For purposes of the Program, “customer information” means any non-public personal information about a customer of the site, or information the site receives about the customer of another financial institution that can be directly or indirectly attributed to the customer. This Program, in and of itself, does not create a contract between the site and any person or entity.

Program Purposes

- Ensure the security and confidentiality of the customer information contained within the website located at <https://secure.dmsintegration.com> (the site);
- Protect against any anticipated threats or hazards to the security and/or integrity of the said customer information; and
- Protect against unauthorized access to or use of the site’s customer information that could result in substantial harm or inconvenience to any customer

Program Coordinator(s)

This Program and the safeguards it completes shall be implemented and maintained by an employee or employees (“Program Coordinator”) designated by the site. The Program Coordinator shall design, implement and maintain new safeguards as he or she determines to be necessary from time to time. The Program Coordinator shall report to the President. The Program Coordinator may delegate or outsource the performance of any function under the Information Security Program as he or she deems necessary from time to time.

In the event the Program Coordinator leaves the employment of the site, the President shall take over the responsibilities of the Program Coordinator until a new Program Coordinator is designated.

Risk Assessment

The Program Coordinator shall conduct a risk assessment to identify and evaluate reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in its unauthorized disclosure, misuse, alteration, destruction or other compromise of customer

information or information systems, assess the likelihood and potential damage of these threats taking into consideration the sensitivity of customer information and evaluate the sufficiency of existing policies, procedures, customer information systems and other safeguards in place to control risks.

The risk assessment shall cover all relevant areas of the site's operations, as determined by the Program Coordinator. At a minimum, the risk assessment shall cover the following:

- Employee training and management;
- Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
- Detecting, preventing and responding to attacks, intrusions or other systems failures.

Once the Program Coordinator has identified the reasonably foreseeable risks to the site's customer information, the Program Coordinator will determine whether the site's current policies and procedures in these areas sufficiently mitigate the potential risks identified. If not, the Program Coordinator shall design new policies and procedures that meet the objectives of the Program shall be made part of the Program.

Audit

The Program Coordinator shall regularly test or audit the effectiveness of the site's safeguards' key controls, systems, and procedures, to ensure that all safeguards implemented as a result of the risk assessment are effective to control the risks identified in the risk assessment. The Program Coordinator shall revise current safeguards and/or implement new safeguards as necessary to ensure the continued viability of the Program.

Overseeing Service Providers

The Program Coordinator shall be responsible for overseeing the site's service providers who handle or have access to customer information. The Program Coordinator shall take reasonable steps to select and retain service providers that are capable of maintaining safeguards to protect the specific customer information handled or accessed by each service provider that are consistent with the level of safeguards employed by the site for such information.

The Program Coordinator shall review and approve each service provider contact prior to its execution by the site to ensure that each contact contains appropriate obligations of the service provider to comply with the site's safeguarding requirements. The Program Coordinator will ensure that such providers are required to comply with this Information Security Program, and monitoring such provided for compliance herewith.

Periodic Reevaluation of the Program

The Program Coordinator shall reevaluate and modify the program, as necessary, from time to time as the Program Coordinator deems appropriate. The Program Coordinator shall do as such reevaluation and modification on the following:

- The results of the Program Coordinator's testing and monitoring efforts;
- Any material changes to the site's operations, business or information technology arrangements; and
- Any other circumstances that the Program Coordinator knows, or has reason to know, may have a material impact on the Program, including changes to technology, sensitivity of customer information, reasonably foreseeable internal or external threats to customer information, changes to our own business (such as mergers or acquisitions or outsourcing) and/or changes to customer information systems.

In order to assist the Program Coordinator in this regard, the site shall keep the Program Coordinator apprised of the nature and extent of all third party relationships and any operational changes or other matters that may impact the security or integrity of the site's customer information.

Information Security Policies and Procedures Employee Training and Management

In keeping with the objectives of the Program, the site shall implement, maintain and enforce the following employee management and training safeguards:

- 1. All employees and independent contractors are responsible for complying with the site's Program.*
- 2. The site will check references of each potential employee prior to the commencement of the applicant's employment.*
- 3. The site will obtain a consumer report and criminal background check of each applicant prior to the commencement of the applicant's employment.*
- 4. All offers of employment shall be subject to satisfactory references and consumer/criminal report investigations.*
- 5. All new employees and independent contractors who perform services in the site that have access to customer information will participate in the site's information security training. Each person shall sign and acknowledge his or her agreement to abide by the site's Program. Training will recur at least once each year or sooner as determined by site management and as required by changes to the Program.*

6. *Such training program shall include, at a minimum, basic steps to maintain the security, confidentiality and integrity of customer information, such as:*
 - *Identifying for employees and independent contractors the types of customer information subject to protection under the Information Security Program.*
 - *Locking rooms and file cabinets where paper records are kept.*
 - *Using password-activated computer software, systems, applications or terminals or an automatic log-off function that terminates access after a short period of inactivity.*
 - *Using strong passwords (at least eight characters long and alphanumeric).*
 - *Changing passwords periodically, and maintaining the security of passwords.*
 - *Sending electronic information over secure channels only.*
 - *Appropriately disposing of paper and electronic records.*
 - *Other training as determined appropriate by site management from time to time.*
7. *The site will take appropriate steps to encourage awareness of, and compliance with the Program.*
8. *All employees and independent contractors will be permitted to access customer information on a "need-to-know" basis as determined by site management.*
9. *Personnel shall not be permitted to access, use or reproduce customer information, whether electronic or non-electronic, for their own use or for any use not authorized by the site.*
10. *All persons who fail to comply with the site's Program shall be subject to disciplinary measures, up to and including termination of employment for employees or contract termination for independent contractors that perform services in the site. This remedy shall be expressly provided for in site's agreements with such independent contractors.*
11. *Upon termination of an employee or independent contractor, that person's physical and electronic access to customer information shall be blocked, including the deactivation of their passwords and user names.*

Information Security Policies and Procedures - Information Systems

In keeping with the objectives of the Program, the site shall implement, maintain and enforce the following information systems safeguards:

1. *The amount of customer information collected shall be limited to the amount reasonably necessary to accomplish the legitimate business purpose of the site, or to comply with state or federal regulations.*
2. *All records containing customer information shall be stored and maintained in a secure area.*
 - *Paper records shall be stored in a room, cabinet, or other container that is locked when unattended. The Program Coordinator shall control access to such areas.*
 - *All storage areas shall be protected against destruction or potential damage from physical hazards, like fire or floods.*
 - *Electronic customer information shall be stored on secure servers. Access to such information shall be password controlled, and the Program Coordinator shall control access to such servers.*
 - *Unique User IDs and other identifiers used to access electronic customer data shall be assigned and managed by the Program Coordinator.*
 - *Customer information consisting of financial or other similar information (e.g., name, address, etc.) shall not be stored on any computer system with a direct Internet connection.*
 - *To the extent technically feasible, customer information that may be stored on laptops or other portable media shall be encrypted.*
 - *All customer information shall be backed up on a daily basis. Such back up data shall be stored in a secure location as determined by the Program Coordinator.*
3. *All electronic transmissions of customer's information, whether Inbound or Outbound, shall be performed on a secure basis.*
 - *Inbound sensitive user and financial data transmitted to the site directly from users shall use a secure connection, such as a Secure Sockets Layer (SSL) or other currently accepted standard, so that the security of such information is protected in transit. Such secure transmission shall be automatic. Users shall be advised against transmitting sensitive data, like account numbers, via electronic mail.*
 - *The site shall require by contract that inbound transmissions of customer information delivered to the site via other sources be encrypted or otherwise secured.*
 - *All outbound transmissions shall be secured in a manner acceptable to the Program Coordinator.*
 - *To the extent sensitive data must be transmitted to the site by electronic mail, such shall access at the discretion of the Program Coordinator.*

- *The Program Coordinator shall review all vendor applications to ensure an appropriate level of security both within the site's business partners and vendors.*
4. *All paper transmissions of customer information by the site shall be performed in a secure manner.*
 - *Sensitive customer information shall be properly secured at all times.*
 - *Customer information delivered by the site to third parties shall be kept sealed at all times.*
 - *Paper-based customer information shall not be left unattended at any time it is in an insecure area.*
 5. *All customer information shall be disposed of in a secure manner.*
 - *The Program Coordinator shall supervise the disposal of all records containing customer information.*
 - *Paper based information shall be shredded and stored in a secure area until a disposal or recycling service picks it up.*
 - *All hard drives, diskettes, magnetic tapes, or any other electronic media containing customer information shall be erased and/or destroyed prior to disposing of computers or other hardware.*
 - *All hardware shall be effectively destroyed.*
 - *All customer information shall be disposed of in a secure manner after any applicable retention period.*
 - *The length of time customer information is retained shall be limited to the time reasonably necessary to accomplish the business purpose of the site or to comply with state or federal regulations.*
 6. *The Program Coordinator shall maintain an inventory of the site's computers and storage media, including any laptops, handheld devices or PDA's on or through which customer information may be stored, accessed or transmitted.*
 7. *The Program Coordinator shall develop and maintain appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information and document any actions taken in connection with any breach of security. Such procedures shall include a post-incident review of events and actions taken to improve security.*

Information Security Policies and Procedures - Detecting, Preventing and Responding to Attacks, Intrusions or Other Systems Failures

In keeping with the objectives of the Program, the site shall implement, maintain and enforce the following attack and intrusion safeguards:

1. *The program Coordinator shall ensure the site has adequate monitoring and procedures to identify and address any breaches of the site's information safeguards that would materially impact the confidentiality and security of customer information. The procedures shall address the appropriate response to databases and computer systems, etc.*
2. *The Program Coordinator shall utilize and maintain a working knowledge of widely available technology for the protection of customer information.*
3. *The Program Coordinator shall communicate with the site's computer vendors from time to time to ensure that the site has installed the most recent patches that resolve software vulnerabilities.*
4. *The site shall utilize anti-virus software that updates automatically.*
5. *The site shall maintain up-to-date firewalls.*
6. *The program Coordinator shall manage the site's information security tools for employees and pass along updates about any security risks or breaches.*
7. *The Program Coordinator shall establish procedures to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure.*
8. *The Program Coordinator shall ensure that access to customer information is granted only to legitimate and valid users, and that such access is removed from any inactive users or inactive accounts.*
9. *The Program Coordinator shall notify customers promptly if their customer information is subject to loss, damage or unauthorized access.*