Version 3.0
11/18/2024

DATA SECURITY POLICY

DATA SECURITY POLICY

Introduction

The Data Security Policy (DSP) provides definitive information about the prescribed measures used to establish and enforce the Information Security Program at OlerRelo Group. OlerRelo Group is committed to protecting its employees, partners, customers, and agents from damaging acts, either intentional or unintentional. Security is a team effort involving the participation and support of everyone who interacts with data and information systems. Therefore, it is the responsibility of every user to know these policies and to conduct their activities in accordance with these policies. It is critical that we protect information we collect about clients, partners, and other agents. The security of data and information systems must include controls and safeguards to offset possible threats, reduce exposure to risk, and ensure the confidentiality, integrity, and availability of data. Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and information systems; this includes accidental loss or destruction.

Purpose

The purpose of the DSP is to prescribe a comprehensive framework for:

- Protecting the confidentiality, integrity, and availability of Oler Relo Group data and information systems
- Protecting Oler Relo Group, its employees, clients, and agents from illicit use of Oler Relo Group information systems and data
- Ensuring the effectiveness of security controls over data and information systems that support OlerRelo Group's business operations
- Recognizing the highly networked nature of the current computing environment and provide effective enterprise-wide management and oversight of those related information security risks.
- Providing for development, review, and maintenance of minimum security controls required to protect Oler Relo Group's data, information systems, and business operations.

Implement consistent security controls across all systems processing our data, Inclusive of agent locations and third-party supply chain partners, will help us comply with current and future legal obligations to ensure long term due diligence in protecting the confidentiality, integrity, and availability of Oler Relo Group data.

Scope and Applicability

These policies, standards, and procedures apply to all OlerRelo Group data, information systems, activities, and assets owned, leased, controlled, or used by OlerRelo Group, its agents, contractors, or other business partners on behalf of OlerRelo Group. These policies, standards, and procedures apply to all OlerRelo Group employees, contractors, sub-contractors, and their respective facilities supporting OlerRelo Group business operations, wherever OlerRelo Group data is stored or processed, including any third party contracted by OlerRelo Group to handle, process, transmit, store, or dispose of OlerRelo Group data All personnel supporting or processing OlerRelo Group business functions shall comply with the DSP. OlerRelo Group business units, partners, or agents may create and use a more restrictive policy, but not one that is less restrictive, less comprehensive, or less compliant than this policy. This policy does not supersede any other applicable law, existing labor management agreement, or government regulation in effect as of the effective date of this policy.

Violations

Personnel supporting or processing OlerRelo Group business that are found to have violated the DSP will be subject to disciplinary action, up to and including termination of employment and/or termination of association with OlerRelo Group. Violators of local, state, Federal, and/or international law will be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Information Security Program

OlerRelo Group shall protect the confidentiality, integrity, and availability of its data and information systems. Security controls will be tailored accordingly so that cost-effective controls can be applied appropriately with the risk and sensitivity of the data and information, in accordance with all legal obligations.

Management Commitment to Information Security

OlerRelo Group management is committed to the protection of information assets. Management demonstrates its commitment to information security through its adherence to the following fundamental principles:

- Treating information as a critical business asset.
- Incorporating high standards of corporate governance to all data elements stored, processed and transmitted.
- Demonstrating to customers and business partners that the enterprise deals with information security in a professional manner.
- Ensuring that the enterprise has a set of security policies that implement controls over information and systems that addresses confidentiality, integrity, and availability. Management further demonstrates its commitment to information security by engaging in the following actions:
- Assigning overall responsibility for information security to a member of senior management.
- Allocating dedicated organizational resources to information security.
- External review (third party) of the IS policies to ensure they are meeting or exceeding industry best practices.

Organization of Information Security

The authority and responsibility for managing the information security program are delegated to OlerRelo Group's Information Security Officer (ISO) who has responsibility for:

- Establishing, documenting, and distributing information security policies, procedures, and guidelines.
- Defining, implementing, and supporting a set of security services which provide a range of security capabilities.
- Providing expert advice on all aspects of information security.
- Overseeing the investigation of information security incidents.
- Escalate security alerts to appropriate personnel.
- Contributing to information security awareness programs and developing security skills for staff.

- Evaluating the security risks and implications of business initiatives and procurement of services.
- Working cooperatively with internal and external auditors in the auditing of security practices.
- Partnering with internal groups that have related responsibilities (i.e., Law, Treasury/Audit, Human Resources).
- Monitoring and analyzing security alerts and information.
- Reviews standards for applicability
- Revises standards to address organization changes

General Awareness and Training of Information Security

Specific activities are undertaken to promote security awareness to all associates who have access to information and systems that are supporting OlerRelo Group business. These activities are:

- Endorsed and promoted by management.
- Delivered as part of associate new-hire orientations and as part of on-going associate training.
- Aimed at providing associates with specific expectations of their role in securing, protecting, and handling information.
- Aimed at reducing the frequency and magnitude of information security incidents.
- Role-based security related training will occur before authorizing access to data or systems required for assigned job duties.

Identification of Information Security Controls

OlerRelo Group uses the following sources for the identification of security requirements:

- Risk assessments
- Internal and external penetration tests
- Internal and external vulnerability assessments
- Statutory, regulatory, and contractual requirements that OlerRelo Group must satisfy.
- Principles, objectives, and business requirements for information handling that OlerRelo Group has developed to support its operations.

Assessments

The results of risk assessments, vulnerability assessments, and penetration tests assist in identifying threats to assets, vulnerabilities and the likelihood of occurrence, and potential estimated business impact. These assist in determining appropriate management action, priorities for managing risks, and implementation of controls selected to protect against these

risks, vulnerabilities, and business impact. The following represents OlerRelo Group's approach to information security risk assessment:

- The scope of assessments can be either the whole organization, parts of the organization, a specific information system, or a specific component of an information system.
- Assessments will have a clearly defined scope in order to be effective and will include relationships with risk assessments from other areas as appropriate (i.e., Law, Human Resources, Finance, etc.).
- Assessments may be performed internally, by a third-party, or a combination of both.
- Expenditures on controls to address risk will be balanced against the business harm likely to result from security failures.
- Before considering the control of a risk, criteria will be established for determining whether or not the risk can be accepted. Risks may be accepted if, for example, it is assessed that the risk is low or that the control is not cost-effective for the organization. Such decisions should be recorded.
- Assessments shall be conducted, at minimum, annually.

Data Classification and Handling

Determining how to protect and handle data and information depends on the type of information, importance, and usage. Classification is necessary to understand which security practices and controls should be applied to the data in order to provide the appropriate level of protection. The more sensitive the data, the tighter the controls need to on that data. All data is classified as Public, Proprietary, Restricted, and Highly Restricted as defined in Appendix 1. Data should be handled according to its classification. Specialized data handling procedures may be required for Restricted or Highly Restricted data; in addition, specific customer data may have additional handling instructions that OlerRelo Group has agreed to contractually. Prior to handling or processing data, users should ensure they understand the proper and/or required handling procedures and are following them appropriately.

Legal, Regulatory, and Contractual Compliance

OlerRelo Group will ensure compliance with relevant statutory, regulatory, and contractual requirements affecting information security. The information security organization will work collaboratively with other OlerRelo Group entities, including Legal, Risk Management, Human Resources, and Contracts to evaluate the applicability of OlerRelo Group information security controls to new and existing legislation or regulatory requirements.

Audits and Reviews of Information Security Controls

Information security controls are periodically monitored, reviewed, and improved to ensure that the specific security and business objectives of OlerRelo Group are met. Thus, information security conditions and policies of OlerRelo Group are subject to annual internal and independent audits or reviews. Security audits or reviews are:

- Performed by individuals who have sufficient technical skills and knowledge of information security disciplines.
- Focused on ensuring that information security controls function as intended and are effective enough to reduce risk to an acceptable level.
- Provided to management so that risks can be remediated, or controls can be modified.

Access Control

Access controls are designed to reduce the risk of unauthorized access to OlerRelo Group data and to preserve and protect the confidentiality, integrity, and availability of OlerRelo Group systems. All assigned access shall be reviewed and audited for accuracy to ensure employees only have access to the data required for them to perform their assigned operational duties; access to Restricted or Highly Restricted data shall be audited at a minimum quarterly.

User Access Management

The Security Administration team is responsible for ensuring proper user identification and authentication management by enforcing a formal, documented, provisioning and de-provisioning procedure as follows:

- Centralized control regarding addition, deletion, and modification of user accounts and credentials to ensure authorized use is maintained.
- Verifying user identity and receiving appropriate management before creating or modifying accounts.
- Immediately revoke access for any terminated user.
- Disable or remove inactive accounts at least every 90 days.
- Limit repeated access attempts by locking out an account after no more than six failed attempts. • Require an administrator to unlock any disabled account.
- Track and monitor role assignments for privileged user accounts.
- Enable accounts used by vendors for remote access only during the time period they are needed.
- Ensure assigned access provides adequate separation of duties for all employees

Least Privilege

The principle of “least privilege” access, which states only the minimum level of access will be granted to perform the assigned operational duties, shall be used when granting employees

access to systems or data. Access shall not be granted without an approved business requirement and management approval. Access to Restricted or Highly Restricted data may also require an additional level of approval from the data owner.

Identification and Authorization

Each individual employee is provided a unique user identity for the purpose of identification, authorization, and authentication to systems processing OlerRelo Group data or supporting OlerRelo Group business functions. This unique identity, associated credentials, and password, is considered Highly Restricted information and should only be used by the individual it is assigned. Sharing of unique user identities, associated credentials, or password is not permitted. In the event of a locked account, individuals are only permitted to request their unique account to be unlocked and the individual's identity will be verified prior to the account being unlocked.

Password Management

Passwords are considered Highly Restricted information and therefore, should not be written down or stored in an unencrypted format. Passwords, password complexity, and password lifecycle should, at a minimum, adhere to current industry best practices. Forbidden actions related to passwords include, but not limited to, the following:

- Do not use default vendor passwords
- Do not reveal a password over the phone to anyone
- Do not send your password to anyone via email
- Do not share or tell your password to others
- Do not write your password down

Operational Security

Operational security processes are used to identify critical data and information, the vulnerabilities associated with them, and to determine the appropriate risk mitigations that are needed to ensure OlerRelo Group operations are not negatively impacted.

System Hardening

System hardening procedures should be defined and followed for all systems and platforms (workstations, servers, databases, etc.), both production and development, to reduce the risk of systems being compromised. These procedures should be consistent with industry-accepted hardening standards and include, but not limited to:

- Procedures and standards updated as new vulnerabilities are identified
- Applied when new systems are configured, prior to being connected to the production network
- Follow the 'least privilege' access model
- Remove unnecessary functionality
- Implementing security features as relevant (SSH, TLS, etc.)
- Removal of all default vendor accounts and passwords
- Installation of anti-virus software where feasible
- Appropriate level of monitoring and logging is enabled and retained to allow review after a service impacting event is encountered

In addition to the above hardening standards, the following steps shall be taken to further protect systems and reduce risk:

- Establishing owners of each system and assigning responsibility to personnel that are technically capable
- Ensuring that privileged access to systems is restricted to authorized personnel only
- Following defined access management procedures when generating system access
- Designing systems to operate with current and predicted load levels
- Separating production and testing systems
- Limiting the use of production data in test environments when possible
- Monitoring and supervising the activities of personnel responsible for systems
- Ensuring the appropriate level of replication and/or backups are configured
- Using industry accepted levels of encryption for data at rest, transit, and processing when technically feasible
- Identifying end of life components and planning appropriately for migrations to supported versions prior to end of support/life
- Ensuring the appropriate level of redundancy is configured and available to reduce single points of failure
- The installation of software on systems is restricted to authorized personnel only
- Processing and storage capacity planning is conducted appropriately to ensure business growth needs are met
- Where possible, automated system provisioning and deprovisioning processes will be implemented to reduce the occurrence of hardening variations
- Appropriate use of firewalls, intrusion detection, and intrusion prevention, and log aggregation systems

Patch Management

Routine installation of vendor-issued updates and patches (operating system, security, etc.) are necessary to protect systems and data from compromise and erroneous function. All systems (workstations, servers, network devices, firewalls, routers, mobile devices, etc.) should routinely and regularly have patches installed. At a minimum, general patches should be installed quarterly while critical security patches should be applied as soon as possible. Proper

testing of patches in a test environment, prior to release on production systems, is crucial to ensure interruptions to operations is not encountered.

Change Control

Change control processes are followed to maintain the integrity of production and non-production systems, to ensure that standardized methods are used for handling of all changes, and to minimize the impact of change related incidents. A defined and documented change management process should be followed that includes, at a minimum, the following:

- Logged change request
- Prioritization of the change
- Documentation of the impact
- Documented approval for the change
- Functionality testing to verify the change does not have a negative impact
- Back-out procedures

Asset Management

OlerRelo Group personnel, business partners, agents, and contractors shall protect assets associated with OlerRelo Group operations by ensuring appropriate handling requirements are followed to prevent unauthorized disclosures regardless if assets or data are being stored or transmitted. All assets associated with data or with data processing shall be inventoried and tracked. The inventory shall include, but not limited to:

- A list of all devices
- Method to accurately and quickly determine the owner
- Contain contact formation for the asset owner
- Be updated promptly as necessary

Physical Security

A defined and documented physical security program and procedures shall be used to ensure the physical protection of all systems associated with OlerRelo Group business. The physical security program shall include, but not limited to:

- Security perimeters should be defined and used to protect areas that contain OlerRelo Group data or systems
- A list of personnel with authorized access to the facility and promptly remove access as necessary
- Use of access control mechanisms (access badge, biometrics, etc.) where possible
- Issue authorization for physical access
- Strictly limit access to sensitive areas and/or areas that contain systems processing OlerRelo Group data
- Use video cameras and other recording and/or logging devices when possible
- Register and log all visitor access to the facility

Disaster Recovery and Business Continuity

Disaster Recovery (DR) and Business Continuity (BC) refers to responding to an operational interruption through the implementation of a recovery plan. The recovery plan accounts for applications deemed critical for business operations, service delivery, and ensures the timely restoration of OlerRelo Group's capability to deliver services. The DR/BC plan should be tested, at minimum, annually to ensure the plan is up to date and capable of sustaining business operations during a period of disruption. OlerRelo Group, and those conducting OlerRelo Group business shall:

- Develop a contingency plan for business-critical systems that
    - Provides recovery objectives and restoration priorities
    - Determines contingency roles, responsibilities, and assigned individuals
    - Addresses maintaining essential business functions during a disruption
    - Addresses full system restoration o Is reviewed and approved by designated company officials
- Communicate contingency plan throughout the organization and ensure assignments are understood
- Coordinate contingency planning and plan reviews at least annually
- Modify the plan accordingly to address business changes
- Establish procedures to access data and systems during periods of disruption
- Ensure defined plans and procedures meet and adhere to contractually obligated recovery timelines and/or objectives

Incident

Response Incident response refers to the actions taken to address an event that either creates service disruption or impacts a customer and incidents can range from minor to business crippling in scale. Incident response procedures should be periodically reviewed to ensure the defined steps are current and applicable to the existing environment. In order to have an effective response to an incident, there must be a defined, repeatable process that is followed.

OlerRelo Group addresses incident response by applying these main steps to all encountered incidents:

- Preparation - Ensuring staff are properly trained and know what steps to take
- Identification and Prioritization - Determine that an incident has occurred, and assign the priority/urgency
- Containment - Isolate the impacted items to prevent additional damage

- Neutralization - Remove the disruption from the environment and perform root cause analysis
- Recovery - Return impacted items to normal operations
- Lessons Learned - Determine ways to prevent the incident from reoccurring

Software Development Life Cycle

A Software Development Life Cycle (SDLC) is a series of steps that provides a framework for developing and managing software throughout its life cycle. When implemented correctly, a SDLC ensures that that highest quality software is delivered in a quick time, for the lowest overall cost. All development activities at OlerRelo Group follow a defined SDLC which takes into account the following items:

- Plan
- Build
- Test
- Deploy
- Maintain

During this process, attention is given to clearly identify the functionality requirements, remedy the code of vulnerabilities and bugs, ensure it meets the stakeholder's needs, and is safe to deploy into the production environment. The SDLC is followed for all feature enhancements, upgrades, etc. until the product is discontinued and removed from service.

Acceptable Use

Employees are granted access to OlerRelo Group equipment and systems in order to assist them in performing their job. The equipment and systems belong to OlerRelo Group and use is intended only for legitimate, business purposes. Employees should not have an expectation of privacy in anything they create, store, send, or receive on OlerRelo Group systems or equipment. Without prior notice, OlerRelo Group may review any material created, stored, sent or received on its systems or equipment. All employees using OlerRelo Group systems or equipment are obligated to use these items responsibly, professionally, ethically, and lawfully.

Equipment and System

Usage Users shall:

- Immediately report: all lost or stolen equipment, known or suspected privacy or security incidents
- Log off or lock systems when leaving them unattended
- Completed all required security and privacy training

- Follow appropriate data handling procedures
- Be vigilant when access the internet and verify all material safe before viewing
- Follow the “Clean Screen, Clean Desk” mentality to protect sensitive data, to include customer data
- Follow all defined record retention policies
- Only connect to known and trusted networks
- Speak only for yourself on social media accounts as you could mistakenly be viewed as a spokesperson for OlerRelo Group in your online communications.
- Only use OlerRelo Group systems and equipment for their intended business purpose
- Adhere to OlerRelo Group’s privacy policy, code of conduct, and data security policy
- Only use customer data for the purpose it was collected and in accordance with OlerRelo Group’s privacy policy
- Report all policy violations to: info@olerrelo.com

Users shall not:

- Copy or store sensitive/proprietary information or customer information on removal media devices
- View material that is: sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, defamatory, or otherwise unlawful in nature
- Download material or software from the internet or unknown sources
- Install software on OlerRelo Group systems or equipment OlerRelo Group, C.A. Data Security Policy
- Modify, revise, transform, or adapt any OlerRelo Group software install on equipment and systems
- Transfer OlerRelo Group or OlerRelo Group customer data through any unsecure network
- Use any utility program which allows the circumventing of OlerRelo Group applied controls
- Send unsolicited emails or send spam emails
- Use OlerRelo Group systems or equipment for any activity that violates local, state, federal, or international law
- Introduce any malicious software (virus, trojan, malware, etc.) into or onto OlerRelo Group systems or equipment
- Use OlerRelo Group equipment or systems in support of “for-profit” activities or outside employment/business activity (such as consulting for pay, sale of goods, etc.)
- Use OlerRelo Group systems or equipment for malicious activities
- acquire, use, reproduce, transmit, or distribute any controlled information including computer software and data that includes information subject to the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export-controlled software or data
- Remove OlerRelo Group systems or equipment from the organization without prior management approval

- Post information on social media sites or other public forums which: are derogatory to OlerRelo Group or its management, contrary to OlerRelo Group's code of conduct and mission, or brings discredit to OlerRelo Group

Record Retention

Information created, received, or maintained in the transaction of OlerRelo Group business, whether in paper or electronic form, is considered a formal record and is subject to OlerRelo Group's Control of Record Procedure. This procedure defines the process for identification, storage, protection, retrieval, retention, hold, and disposition of records. OlerRelo Group will not keep personal information in a form that permits identification of data subjects for longer than necessary for the purposes for which it was collected or to which the data subject has consented, except for legitimate purposes permitted by law, such as regulatory compliance. All record disposal will follow OlerRelo Group Derelict Media Collection and Destruction Process.

Teleworking

Associates identified as critical to business continuity will have the ability to work remotely. In addition, remote working may be a viable alternative work arrangement for some employees. Teleworking is not an entitlement and is not a OlerRelo Group wide benefit. In addition to the acceptable use policy, employees working remotely should take additional precautions to ensure the protection of data by properly securing, both logically and physically, all equipment, data, and communications.

Special Topics

This section is reserved for additional topics.

Vendor Management

Vendors, third parties, and supply chain partners will be held to the same standards contained within OlerRelo Group's Data Security Policy, Privacy Policy and Code of Conduct. Additionally, they may be required to meet customer contractual controls if/when processing customer data. Audits will be conducted on these parties as applicable to ensure compliance is met and the required protections are provided. Relationships with vendors, third parties, and supply chain partners will be governed by mutually accepted contractual requirements.

Procurement

The procurement of new systems and software will follow a defined process in order to ensure an unbiased and comprehensive review of offering is conducted prior to purchase. The review

process will specifically include a data security review to ensure the offering has appropriate security controls and features.

Appendix 1

All information assets are assigned a sensitivity level based on the data element's level of sensitivity, value, and criticality to OlerRelo Group, its customers, agents, contractors, or business partners. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data elements are to be assigned one of the following four sensitivity levels:

	Definition	Potential Impact of Loss
HIGHLY RESTRICTED	Highly Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Highly Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.	SIGNIFICANT DAMAGE would occur if Highly Restricted information were to become available to unauthorized parties either internal or external to OlerRelo Group. Impact could include negatively affecting OlerRelo Group's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
RESTRICTED	Restricted information is highly valuable, sensitive business information and the level of protection is dictated internally by OlerRelo Group and contractual requirements.	MODERATE DAMAGE would occur if Restricted information were to become available to unauthorized parties either internal or external to OlerRelo Group. Impact could include negatively affecting OlerRelo Group's competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
PROPRIETARY	Proprietary information is information originated or owned by OlerRelo Group or entrusted to it by others. Proprietary information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.	MINIMAL DAMAGE would occur if Proprietary information were to become available to unauthorized parties either internal or external to OlerRelo Group. Impact could include damaging the company's reputation and violating contractual requirements.
PUBLIC	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.	NO DAMAGE would occur if Public information were to become available to parties either internal or external to OlerRelo Group. Impact would not be damaging or a risk to business operations.