DataClover's Information Security Policy

Version 1.4

Security Council (securitycouncil@dataclover.com):

Roger Fugett – Head of Technology

Patrick McSherry – President

Table of Contents

VERSION CONTROL

Version	Date	Author(s) / Reviewer(s)	Changes
1.0	09/01/2018	Roger Fugett / Patrick McSherry	Initial Creation
1.1	10/02/2018	Roger Fugett	Identify by name scoped systems
1.2	10/04/2018	Roger Fugett	Feedback from tech team; define and inject Security Council
1.3	01/23/2019	Roger Fugett	Include customer SP users for inactivity annual audit; clarify password change policy requirements;
1.4	02/20/2019	Roger Fugett	Introduce Purpose & Scope; updates to “personnel” throughout

PURPOSE & SCOPE

The purpose of the DataClover Information Security Policy is to ensure the appropriate rules and measures are put into place to secure the information in which DataClover owns or has guardianship over. This policy applies to all personnel (employee, contractor, vendor, etc.) who has access to DataClover assets, whether physical or virtual. Throughout this policy, the term "Personnel" refers to any employee, contractor, or vendor.

ACCEPTABLE USE

Equipment

All equipment that DataClover provides to its Personnel, whether for office or home use, remains the property of DataClover. Use of this equipment must adhere to the guidelines of this Acceptable Use policy. Equipment use that could lead to harm of the company, employees, or customers, is a violation of DataClover company policy and could lead to penalties including termination.

DataClover Personnel must not acquire, possess, trade, or use hardware or software tools that can be used to evaluate or compromise information systems security, unless specifically authorized by a member of the Security Council. Examples of such tools include those which defeat software copy protection, compromise confidential credentials, or identify security vulnerabilities.

Company Supplied Devices

Personnel may not use DataClover, owned or issued, computing equipment to aid in the download, sharing, or illegal transferring of copyrighted or trademarked material either through the use of peer-to-peer or file sharing/torrent websites or software. All DataClover issued mobile devices, including but not limited to laptops and cellphones, must be returned to senior technology management when no longer necessary or to DataClover management upon termination.

BYOD

BYOD (Bring Your Own Device) must not interfere with or harm business activities. BYOD devices brought to work by DataClover Personnel are subject to the same security and privacy policies as DataClover issued devices.

Destruction and Re-Use

Before disposal, donation, return from lease, or recycling, the Technology Team, where applicable, must ensure that Confidential and Highly Confidential information has been, or will be, securely wiped from the device.

Mobile Computing and Teleworking

Personnel possessing a laptop, tablet, smartphone, external drive, or flash drive containing Confidential or Highly Confidential must not leave these devices unattended in public places. When stored in a motor vehicle or in other similar physically semi-secure locations which are left unattended, Personnel should keep all portable computing devices covered and out of sight. For example, when left in a locked car or in an unattended hotel room, these devices should be placed in a car trunk or hotel safe. These devices include, but are not limited to, laptops, smartphones, and tablets.

When traveling by air with an electronic device containing Confidential or Highly Confidential DataClover information, Personnel must not check these computers in airline luggage systems.

A personal computer, laptop, smartphone, or other electronic devices used for DataClover business activities must not be lent to anyone.

When telecommuting, the security of DataClover property at an alternative work site is just as important as it is at the central office. At alternative work sites, reasonable precautions must be taken to protect DataClover hardware, software, and information from theft, damage, and misuse.

Any loss, theft, or tampering of DataClover owned equipment or personally owned equipment used for DataClover business activities, must be immediately reported to the proper authorities, in addition to the Security Council at DataClover.

Software

DataClover Personnel must not accept any form of assistance to improve the security of their computers without first having the provider of this assistance approved by DataClover's Security Council. This means that Personnel must not accept offers of free consulting services, must not download free security software via the Internet, and must not employ free security posture evaluation web pages, unless the specific provider of the assistance has been previously approved by the Security Council.

Data and cloud storage must use DataClover approved solutions which are currently the DataClover Google G Suite *Google Drive* solution and Amazon Web Services' *Simple Storage Solution (S3)* product.

Internet, Email, and Communications

DataClover provides internet connectivity at its Buckhead office. This provided internet access should be used primarily for the purpose of business operations and not to be used for any purpose that might harm the company, its customers, or its employees.

Office email should be used primarily for the purpose of business communications. This access is not to be used for any purpose that might harm the company, its customers, or its employees. By making use of DataClover systems, Personnel consent to allow all information they store on systems used for DataClover business to be divulged to law enforcement at the discretion of DataClover management.

DataClover owns all messages sent over DataClover's electronic mail and messaging systems, including but not limited to Google G Suite, and Slack collaboration services. DataClover Personnel should have no expectation of privacy in these messages, which may therefore be captured, read, and used by DataClover management.

Unacceptable communication and collaboration use are defined as, but not limited to, the statements below:

- Personnel must not send electronic messages modified to deceive the recipient regarding the sender or the content of the message.
- Personnel should not use an electronic account assigned to another individual to either send or receive messages.
- Personnel are prohibited from requesting a customer to reveal his or her password, social security number, financial information, or other sensitive information via regular email.
- DataClover utilizes a centralized email system for all DataClover and affiliate email. Employees must not establish their own decentralized electronic mail servers, use ISP-based web mail services, or otherwise use outside services to circumvent the centralized email filtering process.
- Personnel must not open electronic mail attachments unless they were expected from a known and trusted sender.

Virus Protection and Security Controls

Systems without the required software patches or systems that are virus-infested must be disconnected from any DataClover infrastructure and application services.

Any Personnel who suspects infection by a virus must immediately shut-down the involved computer, disconnect from any DataClover servers and services, and contact the Technology team, and make no attempt to eradicate the virus.

Personnel must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any DataClover computer or servers.

Personally Identifiable Information (PII)

Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII. PII can be sensitive or non-sensitive.

Non-sensitive PII is information that can be transmitted in an unencrypted form without resulting in harm to the individual. Non-sensitive PII can be easily gathered from public records, phone books, corporate directories and websites. Such non-sensitive information may be name, address, and phone number.

Sensitive PII is information which, when disclosed, could result in harm to the individual whose privacy has been breached. Sensitive PII should therefore be encrypted in transit and when data is at rest. Such

information includes biometric information, medical information, personally identifiable financial information (PIFI) and unique identifiers such as passport or Social Security numbers. DataClover does not require the use of Sensitive PII and thus does not collect or store such information.

ACCESS CONTROL

Overview

The purpose of the Access Control Policy is to establish requirements on how to grant access to data that DataClover owns or has guardianship over. This policy applies to all computer and application services owned by or administered by DataClover.

Business Requirements of Access Control

Access Control Policy

DataClover follows and implements RBAC (role-based access controls) and follows the principle of least privilege with regard to access to system resources. Unambiguous, organized, and current records of all production information system access privileges should be maintained in a method accessible only by authorized persons.

Scoped Systems

Access to systems containing DataClover customer data—referred to as Scoped Systems—must be limited to only that which is required for business use. When access to a Scoped System is being requested, a JIRA tickets must be created, and manager approved. Careful review is required to ensure that all sensitive information about customers is accessible only to those DataClover Personnel who need such access in order to perform their tasks.

Scoped Systems include but are not limited to:

GitHub
Amazon Web Services Production Account
VPN Software
DataClover Service Pulse Databases
(development, staging, and production)
DealerVault
CDK
Service Pulse

Accounts and Password Policy

Whenever DataClover configures a system or application account for an employee, contractor, or customer, it should take steps to confirm the identity of the user. Upon creation of a *Scoped System* account, each user ID should default to a unique identity for only one user. Shared or group user IDs should not be created or used unless otherwise approved by the DataClover Security Council. Such request and approval should be captured in a JIRA ticket.

User account passwords for *Scoped Systems* must fulfill the following requirements:

All passwords must meet at least three of the following parameters: uppercase letter, lowercase letter, number, and/or symbol.

All passwords must be at least 8 characters long

All user IDs must have their associated privileges revoked after no more than a twelve-month (365 days) period of inactivity. This includes but not limited to customer user accounts utilized to access the Service Pulse solution.

User IDs which have implemented two-factor authentication should change their passwords at least every 365 days. User IDs which do not have two-factor authentication, must be required to change their passwords at least once every 180 days.

All production business applications supporting multiple personnel must be secured by an access control system. No IT systems are exempted from this control.

Systems and applications that contain sensitive data, such as Sensitive PII, require the employee or contractor to use two-factor authentication to gain access.

Access Management

New Hires

All prospective DataClover employees must receive this Information Security Policy as part of their on-boarding process.

All employees should sign a confidentiality agreement incorporating the Information Security Policies applicable to all employees prior to being issued a User ID permitting access to DataClover systems and applications. If an employee has been working without such an agreement, a signature must be provided as a condition of continued employment.

Separations

All DataClover access privileges, both physical and logical, must be promptly terminated at the time that Personnel ceases to provide services to DataClover. DataClover reserves the right to immediately revoke all rights, privileges, and accesses that have been extended to Personnel who have communicated intent to leave employment. At a minimum, the following should be conducted:

- All physical access rights to DataClover facilities must be terminated and all keys and/or access cards must be collected according to applicable procedures.
- Access rights to DataClover information systems and applications must be terminated.
- All Personnel dismissed in an involuntary termination must have their systems access locked as soon as possible.
- All system privileges for any personnel account ID shown to be engaged in abusive or criminal activity may be revoked and turned over to appropriate law enforcement at DataClover's sole discretion.

Management of Privileged Access Rights

DataClover only permits Administrator access after careful review and wherever it is determined that there is a business need. Privileged access to production environments should be tracked and limited to approved changes and production support situations. Computer and communications system privileges of all personnel, systems, and programs must be restricted based on the need-to-know and must be granted only by a clear chain of authority delegation.

Review of Access Rights

Access reviews for *Scoped Systems* should be reviewed at least annually. A JIRA ticket must be created to track and document the outcome of the access control audit.

Personnel Responsibilities

Use of Secret Authentication Information

DataClover Personnel are responsible for all activity performed with their personal User IDs and must follow appropriate requirements for securing secret authentication information, including:

- Do not use DataClover internal network credentials (User ID and password) on a public internet site that requires authentication.
- Do not permit others to perform any activity with their User IDs
- Do not perform any activity with IDs belonging to other Personnel.

Password Management

DataClover Personnel are accountable for responsible user account and password practices. DataClover will enforce the follow requirements:

- Personnel are expected to protect and secure passwords in compliance with this policy.
- Personnel should not employ any password structure or characteristic that results in a password that is predictable or easily guessed.
- Personnel should immediately change his or her password if the password is suspected of being disclosed or known to have been disclosed to an unauthorized party.
- Personnel should never write down or otherwise record a readable password.
- Personnel passwords must never be in readable form outside a personal computer.
- Personnel passwords should never be shared or revealed to anyone other than the authorized Personnel.
- Personnel should not provide their User IDs and/or passwords to any external parties (specifically including, without limitation, Customers) for any reason, including for the purposes of demonstration of DataClover products and/or technology, without limitation.

Access Control to Program Source Code

Source code shall be monitored and managed with strict change control procedures through established development procedures.

Access to the source code should be restricted to only what is needed to perform appropriate changes and dictated through established change control management procedures.

ASSET MANAGEMENT

Overview

The goal of the Asset Management Policy is to protect and secure the information and IT assets managed by DataClover. This policy provides guidelines for asset responsibility, information classification, and media handling.

This policy applies to any person (associates, contractor, vendor, etc.) who has physical or logical access to Company locations or information assets. This policy applies to all computer and network systems owned by or administered by DataClover.

Responsibility for Assets

Ownership of Assets

DataClover shall assign ownership to its various assets. The owner will bear responsibility and accountability for safeguarding the confidentiality, integrity, and availability of all assets under the owner's control. The owner may delegate responsibility for maintaining the inventory of information systems. Recording of DataClover asset inventory and ownership shall be documented in the Google Drive shared document *DataClover User End-Point Inventory.*

Acceptable Use of Assets

Use of DataClover assets in any manner that could cause harm to the business, customers, employees, or the public is strictly prohibited. Refer to the DataClover Acceptable Use policy for additional information on activity considered to be acceptable and unacceptable use of DataClover assets.

Return of Assets

Upon the end of employment or engagement with the company, all DataClover assets in possession of the Personnel must be returned immediately. Departing Personnel may not retain, give away, or remove from DataClover premises any DataClover Information. All other DataClover Information, including the location of such information, in the custody of the departing Personnel must be provided to the Personnel's immediate supervisor at the time of departure.

Upon the termination or expiration of their contract, all contractors, consultants, and temporaries must give their manager all existing copies, in whatever format, of DataClover Information received or created during the execution of the contract and must identify the location of any such information not under that person's control and certify the destruction of any such information that cannot be located. Any vendors, contractors, consultants, or any third party who may be in possession of a DataClover asset must return the asset within two business days of contract end or the end of business need for the asset. Contractors, consultants, and temporaries may not retain any DataClover information.

Information Classification

Classification, Labeling, Handling of Information

DataClover shall provide information required to allow the Operating Groups to implement and maintain an information asset classification, labeling, and handling program as necessary to effectively safeguard organizational information assets. Assets must be classified by criticality across the organization and consider regulatory, system, continuity, security classification, and business function.

COMMUNICATIONS

Overview

The goal of the Communications Security Policy is to ensure the protection of information in networks and its supporting information processing facilities and to maintain the security of information transferred within an organization and with any external entity.

This policy applies to all personnel (employee, contractor, vendor, etc.) who has physical or logical access to Company locations or information assets. This policy applies to all computer and network systems owned by or administered by DataClover.

Network Security Management

Network Controls

All connections between DataClover internal networks and the Internet—or any other publicly accessible computer network—must include a firewall, security groups, or appropriate logical access controls. Their servers must use encryption to transfer information on public networks between these servers.

All Personnel establishing a connection with DataClover must be authenticated using appropriate methods in line with the Access Control policy.

Security of Network Services

All DataClover network devices including, but not limited to, routers, firewalls, and access control servers, must have passwords or other access control mechanisms. All DataClover computers that can be reached by external party networks must be protected by a privileged access control system.

All wireless access points should be:

- installed, configured, and administered by the DataClover Technology staff
- configured to employ encryption
- placed—and the coverage area designed—so that the possibility of unauthorized signal interception is minimized.

Information Transfer

Information Transfer Policies and Procedures

The Data Management policy and Cryptography policy outline the appropriate methods for DataClover information transfer. Please refer to those policies and established operating group procedure for the secure transmission of information and appropriate communication security. The policies and procedures include the appropriate use of cryptographic techniques to protect the confidentiality, integrity, and authenticity of information, as well as the proper retention and disposal guidelines for business information.

CRYPTOGRAPHY

Overview

The goal of the Cryptography Security Policy is to ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information through guidelines for cryptographic controls and proper key management.

This policy applies to all personnel (employee, contractor, vendor, etc.) who has physical or logical access to Company locations or information assets. This policy applies to all computer and network systems owned by or administered by DataClover.

Cryptographic Controls

Policy on the use of Cryptographic Controls

Encryption should be applied to protect Internal, Confidential, and Highly Confidential information based on the Data Management policy. This standard shall apply to all data in the appropriate categories.

Ciphers in use for encryption must meet, at a minimum, commercially reasonable encryption standards that are commensurate with the sensitivity of data or defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS-140-2. Encryption standards shall be regularly reviewed to verify that appropriate encryption controls are in place.

Data identified as requiring encryption shall be subject to the above encryption standards while at rest. Data in-transit over external or public transfers must use HTTPS for all sensitive personal information, if classified as Highly Confidential per the Data Management policy.

Key Management

Cryptographic private or shared keys, cryptographic secrets, or hashes are classified as Highly Confidential—as outlined by the Data Management policy—and protected using controls defined at that classification level. As such, the following guidelines are recommended to protect encryption keys:

- Access to encryption keys must be restricted by need-to-know with limited Personnel access
- Encryption keys must be revoked once compromised

Loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to a member of the Security Council. They will direct the Personnel in any actions that will be required regarding revocation of certificates or public-private key pairs.

DATA MANAGEMENT

Overview

The purpose of the Data Management Policy is to address the classification, labeling, handling, and retention of DataClover Data with the classification of data into sensitivity levels, guidelines for the control of data based on sensitivity, and data controls to protect the confidentiality, integrity, and availability of data along with relevant retention periods and privacy concerns.

This policy applies to all personnel (employee, contractor, vendor, etc.) who has physical or logical access to Company locations or information assets. This policy applies to all computer and business applications owned by or administered by DataClover.

Information shall be classified and managed in terms of legal, regulatory, and contractual requirements, value, criticality, and sensitivity.

The Data Management policy allows the company to enforce commercially reasonable and/or required security controls in order to protect information from theft, destruction, unauthorized disclosure, unauthorized alteration, and/or tampering by unauthorized Personnel and achieve its business objectives. Personnel should diligently protect all DataClover Internal Use Only, Confidential, and Highly Confidential information.

Data Classifications

All DataClover Personnel must be familiar with the Data Classifications as DataClover Personnel are tasked with identifying, segregating, and handling data accordingly.

Public Data

Definition: Any data intended, expressly authorized, or available for public display or use. Personal Information associated with DataClover's employees, agents, or customers, is never considered "Public data."

Examples of public data:

- Information published on a DataClover or DataClover-affiliated public website or a customer website
- Information presented in other publicly-available forums
- Advertising materials online or in print
- Publicly available information drawn from public sources; e.g. the internet.

Internal Use Only Data

Definition: Any information that (1) is not Confidential or Highly Confidential and (2) is used to run the DataClover business on a day-to-day basis, involving the inner workings of the company, that is relevant, used, and needed by DataClover Personnel in the commission of their duties and responsibilities and which is proprietary.

Examples of Internal Use Only Data:

- Organization Charts
- Meeting presentations or minutes
- Internal operating data (including aggregate data that cannot be traced directly to customers)
- Internal emails that do not describe or contain Confidential or Highly Confidential data
- Non-public promotions
- Business strategy
- Advertising (prior to release)
- Sales data
- Revenue data
- Organizational changes

Confidential Data

Definition: Information that is: (a) identified as confidential by a customer, partner, or DataClover or by contract; (b) that would reasonably be expected to be kept confidential; or (c) that includes personal information which should be kept confidential, but for which unauthorized disclosure would present a relatively low risk of financial harm or identity theft.

Examples of Confidential Data:

- Company financial statements or information, other than financial account information
- Non-Technical Data Flow Diagrams
- Email addresses of Vendors
- Lower-risk personal information: Name **+** (any of the following):
    - Telephone Number
    - Address
    - Photograph

Highly Confidential Data

Definition: Sensitive information that is designated by a customer, partner, DataClover, or by law as appropriate for a high degree of protection. It includes all PII regulated under data privacy laws, or whose disclosure or misuse poses an inherent risk that it could be used to commit identity theft or otherwise harm individuals. Highly Confidential data also includes proprietary technical or financial information tied to DataClover's operations or infrastructure that, if made public, would harm the company from a public relation, financial, or operational perspective.

Functionally, there is not a great degree of difference in how to handle Confidential Data vs. Highly Confidential Data. Confidential Data must be protected and kept confidential. Highly Confidential Data, however, is subject to additional or more stringent controls to prevent its loss or misuse.

Examples of Highly Confidential Data

- Payment card numbers, PINs, Card ID numbers (CAV2/CVC2/CVV2/CID) and name, service code and/or expiration date
- Information regarding DataClover Financial Accounts
- Customer Contracts dealing with Highly Confidential Data, and proprietary information relating to customer business relationships
- Passwords used to access DataClover internal and critical external systems
- Customer Passwords
- Sensitive-PII: *Name + any of the following:*
    - National ID number (incl. Social security numbers) or State ID card number
    - Financial or tax data
    - Date of birth
    - Driver's license number
    - Passport number
    - Political history or affiliations
    - Race/ethnicity/religion
- Any "protected health information (PHI)", as defined by HIPAA

Personnel who have been granted access to Highly Confidential information must not disclose it to any other person without the consent of DataClover's Security Council. Highly Confidential information must be disclosed only after the DataClover's Security Council's explicit authorization has been obtained.

All Highly Confidential Customer information should be encrypted, hashed, or sanitized from records. Unprotected Highly Confidential Information must not be sent via end-user messaging technologies.

Data Control

Data Labeling Process

Standard naming conventions should be utilized.

All files and documents should be labeled according to the most sensitive data classification it contains. The file or document owner shall be responsible for marking the document appropriately. However, in the event a file or document is not marked, Personnel should use reasonable judgment, protect the information according to its likely classification and, if in doubt, treat the information as "Confidential".

Data Handling Process

All data managed by DataClover must be handled in a commercially reasonable manner consistent with the sensitivity and classification of the data.

- Highly Confidential DataClover information, no matter what form it happens to take, must not leave DataClover offices unless under approved controls.
- All Highly Confidential data transported outside DataClover in computer-readable storage (e.g. Laptops, USB, CD, etc.) media must be encrypted using a commercially reasonable encryption algorithm. This includes the use of hard-drive encryption methods on employee and contractor laptops that store Highly Confidential data.
- Computer storage media that has been used to record Highly Confidential information must not leave controlled channels until it has been rendered unusable, according to approved controls.
- All DataClover Personnel handling Highly Confidential information must have secure methods to dispose of such information.
- Encryption employed must meet standards outlined by DataClover Cryptography Policy.

Data Disclosure

All data and information must be assessed for its value, not only to DataClover and its customers, but also to competitors. All requests from an external party for Confidential or Highly Confidential information must be approved by the DataClover Security Council.

Before any external party is given access to DataClover systems, which include Highly Confidential Information that could be accessed by such external party, a contract defining the terms and conditions of such access must be signed by a responsible manager at the external party organization and be approved by DataClover's Security Council.

OPERATIONS

Overview

The goal of the Operations Policy is to outline and direct operational procedures that will ensure the integrity, confidentiality, and availability of DataClover services and data. This includes operational procedures guiding standard information system use, guidelines for malware protection controls,

operational backup guidelines, the logging and monitoring of information systems, controls over operational production software, technical vulnerability management, and controls for the audit of information systems.

This policy applies to all personnel (employee, contractor, vendor, etc.) who has physical or logical access to DataClover locations or information assets. This policy applies to all computer and network systems owned by or administered by DataClover.

Operational Procedures and Responsibilities

Capacity Management

DataClover shall properly manage system capacity to ensure that the availability and integrity of data, infrastructure, and services meets existing and future business needs.

Technology personnel shall use established processes for estimating and monitoring capacity requirements, including those requirements in specifications for systems. Technology owners shall ensure SLAs define capacity requirements and that they are tested and managed for all relevant resources.

Separation of Development, Testing, and Operational Environments

Business application software in development should be kept separate from production application software through physically and/or logically separate computer systems.

Unless technical considerations indicate that it would be excessively costly, Critical production servers should be dedicated purpose machines or virtual machines, running only a single application.

Production applications containing critical business logic should run on multiple servers that have physical access controls, logical access controls, and contingency plans. Contingency plans should include the ability to auto-scale the production environment, redundant critical infrastructure, and storing database backups in different regions than production database location.

Protection

Web Application Firewall

Web application firewall should be deployed to help protect internet web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. Traffic routing and controls defined through security rules should be utilized to help against attacks such as SQL Injection or cross-site scripting.

Backup

Information Backup

All product and customer data required for critical applications operations, must be backed up on a daily basis utilizing separate geographic locations on the AWS platform (availability zones). Archival Media Testing for recovery of critical business information systems should be conducted regularly by means of refreshing the organization's development and staging product environments from prior production backup media.

Control of Operational Software

Installation of Software on Operational Systems

The Technology Team is responsible for the incorporation of software into production environments. Technology owners are responsible for software updates and security concerns for that software, if it is not previously approved for use by DataClover.

Production information systems and its software should be issued by a reputable organization known to have an on-going commitment to providing timely upgrades, patches, and fixes. Every external party software package that DataClover uses for production information systems purposes must be free of deactivation mechanisms that could be triggered by the vendor without DataClover consent.

All custom software to be run on internet facing web servers must be periodically analyzed by web code review tools. All security vulnerabilities discovered by these tools must be corrected as soon as reasonably possible as defined by the Technical Vulnerability Management section of the Operations Security policy.

Technical Vulnerability Management

Management of Technical Vulnerabilities

All DataClover networked production systems must have a process for regularly reviewing and installing all newly released systems software patches, bug fixes, and upgrades. Technology owners in charge of every production information system at DataClover must establish a time period approved by management for the non-emergency periodic installation of patches, fixes, and upgrades to software. Vendor-supplied software patches, fixes, and updates should not be installed on any DataClover production system unless they have first been tested in a development environment.

The Technology Team is authorized to patch software only if the software is downloaded, or otherwise received, from a trusted and recognized source.

Critical patches shall be tested and applied within 30 days.

Restrictions on Software Installation

Software installations onto critical production must be verified by the Technology Team. Software usage and authorization must comply with existing software usage as defined by DataClover information security policies.

FAILURE TO COMPLY

Non-compliance with information security policies, standards, or procedures is grounds for disciplinary actions up to and including termination.