
# Information Security Policy

Version 1.2

# Use of This Document

This document is the confidential information of Classy, Inc. (“Class”). It is intended to be used internally by the directors, officers, employees and agents of Classy Inc. (“**Classy**”) to provide standards, policies, and practices for the handling of information produced or obtained in the course of conducting business. To the extent it is shared with, or disclosed to, clients, potential clients, vendors, or other third parties, the policies, practices, and statements contained herein are transmitted for general informational purposes only. Nothing contained in this document creates a contract or commitment nor shall it amend, modify, augment or supplant any definitive contractual agreement reached between Classy and the relevant third party; moreover, none of the statements contained herein shall be construed to modify or create additional representations or warranties on the part of Classy, unless otherwise stated in the applicable agreement. This will remain the case whether this document is shared before or after the execution of a definitive agreement. Any third party receiving this document acknowledges the foregoing and agrees that the contents of this document are to be kept strictly confidential and not shared with any third party, without the express written consent of Classy.

## Table of Contents

# Overview

## 1.1 Document Administration

| Version | Date | Section | Change Description | Revised By |
|---|---|---|---|---|
| 1.0 | 09/25/2018 | ALL | Initial Version Drafted | Corey Hall |
| 1.1 | 08/05/2019 | 3.3 | Added Engagement Info | Corey Hall |
| 1.2 | 07/15/2020 | 1.4 | Added Chris Himes (COO) | Corey Hall |
| 1.3 | 10/15/2020 | ALL | General Review | Jason Mitchell |

| Publication Date: | 09/25/2018 | Last Review Date: | 10/15/2020 |
|---|---|---|---|
| Approval Body: | Corey Hall, Director of Information Security | | |

## 1.2 Summary

Information produced or obtained by Classy, Inc. (hereinafter, "Classy") in the course of conducting its business is extremely valuable and must be treated as an asset that must be protected from prohibited disclosure, revision, use, or destruction. Prudent and practical steps must be taken to ensure that data integrity, confidentiality of information, and application/data availability are not compromised. Security tools and processes must be implemented and configured to enable adequate and proper restriction of access to programs, data, and other information resources. Physical access measures must also be incorporated and implemented to ensure that only authorized individuals have the ability to access or use information resources. Classy must maintain compliance with Payment Card Industry Data Security Standard ("PCI DSS") Level 1 requirements. All section numbers referenced below refer to the applicable section within the PCI DSS Requirements.

## 1.3 Scope

Information Security may apply to any activity that involves the access to, use, or modification of Classy's information and/or resources. Information Security affects and encompasses Classy's total information and physical environments. The scope or impact is any access, logical or physical, that has the potential to affect Classy in a negative way.

## 1.4 Roles and Responsibilities

Information security is handled by the following individuals per their role and responsibility at Classy defined below. All incidents should be reported to the ISM.

**Classy ISM - Corey Hall**

- Monitor and control access to all data
- Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations
- Establish, document, and distribute security policies and procedures
- Administer user accounts, including additions, deletions, and modifications
- Monitor and analyze security alerts and information, and distribute to appropriate personnel

**Classy Legal - Jason Mitchell**

- Legal holdings and litigation

**Classy COO - Chris Himes**

- Revenue and business operations

## 1.5 Policy Statement

Rights to use Classy's information systems and computing resources must be based on each user's access privileges. Access privileges must be granted on the basis of specific business

needs utilizing the principle of least privilege. Access controls must ensure that even legitimate users cannot access information unless they are authorized to do so. All of Classy's resources, systems and applications will have access controls unless specifically designated as a public access resource.

Classy employees, contractors, and consultants are responsible for participating in maintaining secure access to Classy information systems and computing resources. Classy's management must provide guidance in creating this secure access environment by establishing access management policies, approving roles and responsibilities, and providing consistent coordination of security efforts across the company. The Security Policies and Procedures listed below are approved by management and govern the information environment at Classy.

### 1.6 Policy Updates and Notifications

Classy reserves the right to revise the conditions of this policy at any time. Adequate notification of updates must be provided to all employees. This policy must be reviewed formally, at a minimum, annually and/or when material updates or changes to the environment are made. Employees are responsible for understanding or seeking clarification of any rules outlined in this document and for familiarizing themselves with the most current version of this policy.

## Information Access

### 1.7 Establishing, Changing, & Terminating Information Access

**A. Establishing Access**

A notification of a newly hired employee, temp, or contractor will go to the individuals or departments responsible for establishing the application and systems access required for the new employee to perform his or her job requirements. The notification will only be issued by appropriate personnel.

**B. Employee Position Change**

When an employee changes positions within Classy, a change notification will go to the individuals or departments responsible for establishing the application and systems access required for the employee to perform his or her new job requirements; access must be updated accordingly.

**C. Terminating Access**

When an employee is terminated, whether voluntarily or involuntarily, and exits Classy, a notification must be sent to all applicable parties. The termination notification must be issued immediately upon termination (when the employee no longer requires logical or physical resources) and must be issued by appropriate personnel. Upon receipt of a termination notification, a ticket is automatically generated and all domain and application/systems access is immediately disabled.

## 1.8 System and Application Access

**A. Network Access**

Access to any production system can only occur after an appropriate request is submitted to the Security team with senior management approval. Currently Classy uses Amazon Web Services (AWS) hosted solutions for all of its servers; the physical and technological security measures employed to protect Classy servers are listed immediately below. Information Security must approve any change in schema, provider, or otherwise for Classy's server infrastructure. All network devices within the production environment must be monitored for API changes to the configuration will result in an email that must be received by Classy Information Security. Information Security will validate the change against any recent change tickets and will follow standard incident response procedures if an associated ticket is not found. All authentication attempts and interactive administrative activities to production network devices must be collected and stored for no less than 12 months. Any suspicious activities must be identified based on pre-defined correlations and security alerts must be sent to Information Security, who will respond to the alerts using standard incident response procedures.

Vendor-supplied default passwords must be changed before installing a system on the network (2.1, 2.5).

Any unnecessary default accounts shall be removed or disabled before installing a system on the network (2.1).

For any new components added to the system, configuration standards shall be created and consistent with industry-accepted standards (2.2a).

As new vulnerability issues are identified, these system configuration standards are updated (2.2b).

When new systems are configured, they shall adhere to the system configuration standards (2.2c).

Strong cryptography shall be implemented according to industry standards (2.3d)

Any sensitive authentication data must be deleted upon completion of the authorization process (3.2c).

Access to system components shall be limited to only those individuals whose jobs require such access and shall be issued based on the individual personnel's job classification and function (7.1).

***Physical Security:***

(i) All servers are located in secure Amazon Web Services ("AWS") data processing facilities
(ii) Only data technicians are permitted physical access to facilities; technicians are subject to dual biometric authentication process
(iii) Each employee is subject to extensive background checks
(iv) Continuous video surveillance of all entrances and common areas
(v) Uninterrupted power supply with N+1 redundancy and immediate failover, plus onsite generator

(vi) Dual power paths and multiple network paths with multiple service providers in the event of equipment failure
(vii) Fire suppression systems in place

***Technological Security:***

(i) Dedicated managed firewalls, maintained exclusively by Cloudflare and AWS to protect Classy's application infrastructure
(ii) TLS 1.2 with at least 128-bit encryption on all checkout pages and reporting pages to protect data transmission
(iii) Managed anti-virus protection provided by Classy and powered by Avast, a leader in global IT security
(iv) Avast Anti-Virus protection designed to proactively detect, quarantine, and delete any malware before it executes or reaches endpoint computers on the network.
(v) All passwords encrypted during transmission and at rest in AWS

**B. Application Access**

Access must be based on job requirements, and no user will be granted access beyond what is required to perform day-to-day job responsibilities. All requests for access require appropriate management approval. Access requires a profile including a valid username and password.

General employees are restricted from accessing the application environment and developers from accessing production environments unless explicitly authorized. Promotion of code from test to production environments are performed utilizing proper separation of duties; programmers do not have access to the production code.

*Note: System and user accounts utilized by non-consumer users and vendors to support systems components and applications are to be enabled only during the period of time the vendor requires access. Vendor accounts must be immediately disabled and/or terminated immediately following use. (8.1.5a). While the vendor is remotely accessing the account it will be monitored (8.1.5b).*

## 1.9 Physical Access

**A. Employee Access**

Physical access will only be granted to areas required for employees to perform their job as per or management's specifications. Upon termination of employment, physical access to the premises must be revoked.

For the avoidance of doubt, no Classy employees have physical access to the hosted server environment maintained by AWS. As mentioned above, only AWS data technicians are allowed physical access to server facilities. All technicians go through extensive background checks and are subject to a dual biometric authentication process.

**B. Temporary Access Requests**

Contract and temporary labor will only gain physical access as required by their job

responsibilities and only for so long as those responsibilities persist.

**C. Visitor Access**

All visitors are to be greeted by or escorted to their party. Visitors to limited access areas must be formally authorized by an appropriate Classy employee to access such areas. Visitors to limited access areas must be given a physical token (i.e. a badge) that has an expiration date and that identifies a visitor as a non-employee. Visitors must return their physical token upon leaving a limited access area or at the expiration date.

Visitors must sign a visitor's log prior to being granted physical access to limited access areas. The log must document the visitor's name, the company represented, the authorizing Classy employee, and the date and time of entrance and departure. Unless otherwise restricted or required by law, visitor logs must be retained for at least three (3) months.

## 1.10 Authenticating Users

**A. Unique Systems Users**

All unique usernames assigned to users in order to access Classy information systems and/or computer resources must be unique to each user.

**B. Enforcement**

Users are responsible for all personal account usernames, passwords, tokens, and related personal identification numbers ("PIN"). Classy users are not to share personal account information with any other individual for any reason. Sharing of account usernames, passwords, tokens, and/or PIN pertaining to any Classy systems or applications is strictly forbidden.

**C. Restricted Access Devices**

All Classy information system and/or computer resource usernames will have an associated password and multi-factor authentication ("MFA") to ensure that only the authorized user is able to access and utilize applications and/or systems.

Access to systems that provide identification and access to sensitive areas must be limited to authorized personnel.

Generic passwords or PINs will never be used at Classy**.** After a user's initial login, the user is required to change the password or PIN linked to the user's account for that information system or computer resource. First time passwords must be unique for each user.

**D. Password Policy Settings**

All accounts used by vendors for remote access will only be used during the time period needed and must be monitored when in use.

All users should immediately change their password if they suspect that it has been discovered or used by another. Users must notify Information Security if any access control mechanisms are broken, or if they suspect that these mechanisms have been compromised.

User identity must be appropriately verified before any password, which enables access to a

Classy's information system or network resource is reset.

User passwords must be changed at least every 90 days. Passwords must be at least 7 characters long and include both numeric and alphabetic characters. Password reuse must be restricted to no more than once every 4 uses.

User accounts must be locked after six failed login attempts. The lockout must be for at least 30 minutes or until authorized Classy personnel unlock the account.

Classy employees must not use passwords that are also used for non-Classy accounts.

**E. User Account Review Process**

User accounts that are inactive for more than 90 days on Classy information systems that store, process, or transmit sensitive data must be disabled or removed.

At least every 6 months, appropriate Classy information system owners and/or data custodians or their designated delegates must review and verify logical access rights to Classy information systems and media containing sensitive data. Such rights must be revised as necessary. Inactive accounts over 90 days old must be either removed or disabled.

Classy employees and contractors experiencing a change in status (e.g., termination, position change) must have their logical access rights promptly reviewed, and if necessary, modified or revoked.

## 1.11 Access Methods

**A. Wireless**

All defaults for wireless networks used in Classy offices (e.g., passwords, encryption keys, and SNMP community strings) must be changed before installation. All wireless device security settings are enabled for strong encryption technology for authentication and transmission. All wireless networks employed by Classy in its business operations use the radius protocol and MFA for authentication and transmission.

There are no wireless networks connected to the underlying Classy server environment maintained by AWS.

**B. Remote Access**

Management must approve accounts granting remote access to Classy application servers. All Classy access to application servers must be made through a management host utilizing the SSH protocol.

**C. Mobile Computing**

All portable computing devices used to access Classy information resources must be (i) password protected, encrypted and (ii) compliant with IEEE 802.11b or IEEE 802.11g protocol to access the

Internet.

Personal firewall software must be installed and active on any Classy owned devices with direct connectivity to the Internet that are used to access the Classy's cardholder data environment. The personal firewall software must be configured to specific standards and prevent unauthorized users from altering or disabling it.

Confidential information should not be transmitted to or from a mobile computing device via wireless unless approved wireless transmission protocols along with approved encryption techniques are utilized.

# Vulnerability Detection & Management

## 1.12 Anti-Virus

Anti-virus software must be deployed on all systems commonly affected by malicious software. The anti-virus programs must be capable of detecting, removing and protecting against all known types of malicious software. (5.1)

Periodic evaluations must be performed to identify and evaluate evolving threats by malicious software. All anti-virus software and definitions must be kept current with automatic updates enabled and being performed periodically. These shall generate audit logs which are retained in accordance with PCI DSS Requirement 10.7. (5.2)

Administrator users should not be able to disable or alter the anti-virus. (5.3)

## 1.13 Vulnerability Scanning

Quarterly vulnerability scans against the system components and web application must be performed by a PCI DSS Approved Scanning Vendor ("ACV"). Risk ratings shall be assigned to all vulnerabilities for "high" and "critical" risk items and patches implemented. (6.1)

Vendor supplied security patches will be installed within one month of release by the vendor (6.2).

Following any significant changes to the application or system components, a quarterly vulnerability scan will be performed (11.2.3).

External scans must be rescanned until a passing result is obtained from the ASV (11.2.3).

Internal scans must be rescanned until a passing result is obtained (11.2.1).

Records of remediation activities resulting from the internal and external quarterly vulnerabilities must be maintained. Records include scan reports, change control tickets and/or

other methods of tracking the remediation activities.

### 1.14 Penetration Testing

Penetration testing utilizing the Open Web Application Security Project ("OWASP") methodology shall be performed on an annual basis. (11.3.4) and results stored indefinitely for reference. Any critical, high, and medium vulnerabilities must be mitigated upon review in accordance with our security requirements. Penetration testing will include coverage for the entire CDE perimeter, public web applications and critical systems. Testing from both inside and outside the network will take place to validate any segmentation and scope-reduction controls bi-annually and after any changes to the network architecture. A review considering threats and vulnerabilities experienced in the past 12 months will take place annually. These results are retained indefinitely.

### 1.15 Vulnerability Monitoring

Classy shall maintain a program to monitor and identify new security vulnerabilities using reputable outside sources for security vulnerability information such as NIST, CIS, Ubuntu, and AWS and assign a severity ranking such as critical, high, medium or low.

## Information Handling & Distribution

### 1.16 Classification of Information

All Classy data and information must be categorized into two main classifications (i) Public Information, and (ii) Confidential Information

"**Public Information**" is information that has been declared public knowledge by management and can freely be given to anyone without any possible damage to Classy.

"**Confidential Information**" means all other data and information that is not Public Information. Much of the company's information must be protected very closely, such as client payment data, client transaction data (e.g., personally identifying information of donors and fundraisers), trade secrets, and any other proprietary information vital to the company's success. Sharing of sensitive Confidential Information with a third party will only be undertaken after execution of a contract with sufficient protective provisions regarding the use and non-disclosure of such Confidential Information.

### 1.17 Cardholder and Payment Information

Classy will not store cardholder information on its servers. After a payment card transaction is authorized, the following types of data must never be stored in electronic or non-electronic form by Classy: Magnetic stripe data, CVC2/CVV2/CID/CAV2, PIN/PIN Block.

Cardholder information, including but not limited to, primary account number (PAN), card

verification code and PIN must not be distributed or sent via end-user messaging technologies including, but not limited to, email, instant messaging, chat, unencrypted ftp, etc. in accordance with the PCI DSS (4.2). Classy client data relating to client payment information will not be shared with third parties that are not currently PCI compliant and can attest and prove their current compliance status. (3.2.2, 3.2.3)

In the case that a Primary Account Number ("PAN") is to be displayed back to the user, it shall be masked to only display the last four digits. Only strong cryptographic protocols such as TLS 1.2 and above must be used for end to end communication over any network.

In the case cardholder data is inadvertently stored in any of Classy's system components, procedures must be followed to securely and thoroughly erase cardholder data so that sensitive data cannot be reconstructed.

## 1.18 Handling and Distribution of Data

The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels.

**Minimal Sensitivity:** General corporate information; some personnel and technical information

| | |
|---|---|
| **Access** | Classy employees, contractors, people with a business need to know. |
| **Distribution within Classy** | Standard interoffice mail, approved electronic mail, and electronic file transmission methods. |
| **Distribution outside of Classy** | U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods. |
| **Electronic distribution** | No restrictions except that it is sent to only approved recipients. |
| **Storage** | Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate. |
| **Disposal/Destruction** | Deposit outdated paper information in specially marked disposal bins on Classy premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media. |

**More Sensitive:** Business, financial, technical, and most personnel information

| | |
|---|---|
| **Access** | Classy employees and non-employees with signed non-disclosure agreements who have a business need to know. |

| | |
|---|---|
| **Distribution within Classy** | Standard interoffice mail, approved electronic mail, and electronic file transmission methods. |
| **Distribution outside of Classy** | Sent via U.S. mail or approved private carriers. |
| **Electronic distribution** | No restrictions to approved recipients within Classy but should be encrypted, sent via a private link, or with appropriate privacy and disclosure notices to approved recipients outside of Classy premises. |
| **Storage** | Individual access controls are highly recommended for electronic information. |
| **Disposal/Destruction** | In specially marked disposal bins on Classy premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media. |

**Most Sensitive:** Trade secrets, marketing, operational, personnel, financial, source code, and technical information integral to the success of Classy

| | |
|---|---|
| **Access** | Only those individuals (Classy employees and non-employees) designated with approved access and signed non-disclosure agreements. |
| **Distribution within Classy** | Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods. |
| **Distribution outside of Classy** | Delivered direct; approved private carriers. |
| **Electronic distribution** | No restrictions to approved recipients within Classy but it must be encrypted using FIPS-140 compliant standards. |
| **Storage** | Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer. |
| **Disposal/Destruction** | Strongly Encouraged: In specially marked disposal bins on Classy premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media. |

## 1.19 Client Transaction Data

"**Transaction Data**" for Classy clients (personally identifiable information of persons Classy clients transact with through the Classy application that is stored on Classy servers) may only be

shared directly with the client, and such third party service providers as are necessary to perform the essential functions of the application (e.g., payment processors or hosted server providers). Data may also be used to administer the client's account (to respond to that particular client's questions, support requests, etc.).

In no case will a Classy client be allowed to accept cardholder information, personal medical information, or other similar regulated personal information through the custom questions feature of the Classy application. If asked, Classy employees shall inform clients that they are not allowed to collect such regulated information through the custom question feature. If improper use of this feature is observed, it should be reported immediately to Information Security.

### 1.20 Removable Media

Laptops, flash drives, CDs, disks or other removable media may only be used as authorized by management and only for necessary business purposes. Any employee with Classy data on authorized removable media may be required, at any time, to immediately return or destroy all such data.

### 1.21 Protection of Data

**A. Backups**

Backups of all essential Classy electronically stored business data must be routinely created and properly stored to ensure prompt restoration. Backups of all client data must be made no less frequently than daily.

**B. Environmental**

Adequate environmental controls must be in place and monitored to prevent data loss due to preventable and/or treatable environmental threats.

## Destruction & Disposal of Information

### 1.22 Disposal of Data

**A. Removable Media**

When no longer required, the contents of removable media should be permanently destroyed or rendered unrecoverable in accordance with applicable State, Federal, and company requirements.

**B. Storage Devices**

Prior to disposal or re-use, equipment containing storage media should be cleansed to prevent unauthorized exposure of data. Cleansing procedures should be used that will render all information unrecoverable. An "erase" feature (i.e. putting a document in the desktop recycle bin) is not sufficient.

**C. Printed Material**

When no longer required, all sensitive printed material shall be disposed of by an internal

machine or third-party service that will shred and dispose of all material in the bins on-site on a regular schedule in such a manner that cardholder data *cannot* be reconstructed in accordance with Payment Card Industry Data Security Standard 9.10 and 9.10.1.

**D. Destruction of Media**

Prior to disposal, destroy defective or damaged media (floppy disks, CDs, tapes) containing sensitive information to render the information unrecoverable.

### 1.23 Secure Media Disposal

Dispose of worn, damaged, or otherwise no longer required media in a secure manner. To prevent the compromise of sensitive information through careless or inadequate disposal of computer media, the following controls should be implemented:

(i) Dispose of media containing sensitive information by secure incineration or shredding.

(ii) If planning to reuse magnetic or optical media, completely empty it of data through use of special software designed to securely erase and/or reformat the media. If software is unavailable, reformatting the media a minimum of three times is required.

(iii) Review distribution lists and verify authorized recipients at regular intervals.

## Log Requirements

### 1.24 System & Application Logging Requirements

Automated audit trails for all system components shall be maintained and appropriately stored in accordance with PCI-DSS requirement 10.2, including:

(i) System Logs
(ii) Security Logs
(iii) Security Alerts (from security appliances)
(iv) Application Logs
(v) Network equipment Logs (including firewalls and wireless equipment)
(vi) System errors and corrective actions taken (especially automated error recovery)
(vii) Successful and unsuccessful logins
(viii) Changes to identification and authentication mechanisms-including but not limited to creation of new accounts and elevation of privileges and all changes, additions or deletions to accounts with root or administrative privileges.

Audit logs of all other system components shall be reviewed daily either manually or via SIEM.

Logs must be promptly backed up to a centralized log server and/or media that is difficult to alter.

## 1.25 Security Fault Log

A log of all security faults involving Classy information systems and services is maintained. Faults of any critical security controls must be logged and investigated. Critical security controls must be restored in a timely manner in accordance with the standard incident response procedures ensuring systems are restored to their previous PCI compliant state. Classy will review and investigate exceptions and anomalies identified during the security fault review process.

The following logs and security events shall be reviewed at least daily by Classy SIEM and log monitoring applications.

(i) All security events
(ii) Logs of all system components that transmit cardholder data
(iii) Logs of all critical system components
(iv) Logs of all servers and system components that perform security functions including firewalls, intrusion-detection systems, intrusion-prevention systems and authentication servers.

## 1.26 Log Monitoring

A user event logging system will contain at a minimum the following information in accordance with PCI DSS requirement 10.3:

(i) User ID
(ii) Dates and times of logon and logoff.
(iii) Type of event
(iv) Logon method, location, terminal identity (if possible), Network address
(v) Records of successful and unsuccessful system access attempts
(vi) Records of successful and rejected data access and other resource access attempts
(vii) Name of affected data, system component or resource.

## 1.27 Log Archiving

Audit logs shall be retained for at least one year and the last three months shall be immediately available for analysis. (10.7). Logs and audit trails must be monitored by file integrity or other methods to ensure their integrity. Access to logs must be limited to only those individuals with a need-to-know to protect their integrity.

# Service Provider Requirements

## 1.28 External Service Provider Policy

All service providers should be able to, upon request, provide documentation evidencing their PCI DSS compliance. Classy will maintain a written agreement with each service provider it engages, documenting that service provider's responsibility for protecting any client data that it possesses. (12.8.2, 12.8.3)

## 1.29 Data Transmission

Classy requires all data transmission methods to be reviewed by the Information Security team and at a minimum, requires the TLS v1.2 protocol be used. Further requirements are at the discretion of the security team.

## 1.30 PCI DSS Compliance and Due Diligence

Before engaging a new service provider, Classy will obtain proper documentation of PCI DSS compliance, when applicable. Renewal documentation must be requested from each service provider no less frequently than annually. When evaluating a potential service provider Classy will consider factors such as (i) length of time in business (ii) prior service reputation (iii) current operating capital, and (iv) availability of security audits (12.8.4).

## 1.31 Current Service Providers

A list of all current service providers must be maintained in our list of approved service providers in Confluence or similar shared resource. The specific PCI DSS requirements that are managed by each service provider shall be included in this document (12.8.5).

## 1.32 Classy's Responsibilities as a PCI Service Provider

The legal contracts that Classy signs with its clients must include an acknowledgment that recognizes the responsibility of Classy for the security of cardholder data that Classy possesses, stores, processes or transmits on behalf of the client (12.9).

# Change Management

### 1.33 Network Devices

For all network devices including software firewalls within the Classy Production Environment or allowing access to Classy Production data and/or dataflow, strict change control processes are required.

1. All changes to network infrastructure must have an associated change request (i.e. in JIRA)
2. Change requests require a business case, acceptance criteria, and proof of changes made
3. All changes made in code require two approvers including one lead engineer
4. All major configuration, service, virtual local area network ("VLAN"), and/or access control list ("ACL") changes to network devices should be reviewed by Information Security and functionality testing done to verify change does not adversely impact the security of any system.
5. Back-out procedures must be documented and followed in the event of a failure
6. Any changes to the production environment must be documented in the Classy network diagram.

## Software Development

Classy is dedicated towards the stability, durability, security and overall quality of its software. This dedication requires diligence throughout all aspects of the software lifecycle, including conducting minor changes, and performing significant modifications. Classy shall develop code and maintain systems in accordance to industry security standards and/or best practices. Classy's software-development processes require that pre-production and/or custom application accounts, user IDs, and/or passwords are removed before an application goes into production or is released to clients. Production data (live PAN) must not be used for testing or development.

### 1.34 Code Vulnerabilities

Code vulnerabilities are weaknesses within the programming that might permit unauthorized access to client's data and operational environment. All programming staff are required to be knowledgeable about vulnerabilities in coding that may impact the security of Classy software solutions. Classy shall provide training on a regular scheduled basis to meet this expectation; at a minimum training for software developers must be completed once a year. Specifically, programming staff shall be knowledgeable of information provided by the Open Web Applications Security Project ("OWASP"). Every line of code written by Classy staff is expected to be done with security considerations addressed in accordance to the Payment Card Industry Data Security Standards.

Code will be tested for vulnerabilities at least annually and after any changes by an independent third party specializing in application security. All vulnerabilities must be corrected in accordance with this policy and the application re-evaluated after said corrections are made.

### 1.35 Code Review

Code review processes are an important step in ensuring that software solutions meet security requirements. Code reviews inspect the source code of an application to ensure that the code meets quality standards. They may be manual or automated. Regardless of who and how, code reviews must be performed by an individual(s) other than the originating code author and in accordance to the Payment Card Industry Data Security Standards.

## Security Training and Awareness

### 1.36 Security Awareness Training

Classy must ensure that employees and contractors are provided with sufficient training and supporting reference materials to enable them to appropriately protect Classy's information systems, network resources, and data. Classy must provide information security awareness to its employees and contractors upon hire and then at least annually.

Classy must provide regular security information and awareness to its employees and contractors via methods such as log-in banners, posters, memos, and periodic meetings. Such information and awareness must include, but is not limited to:

- Any significant revisions to Classy’s information security policies
- Significant new Classy’s information security controls or processes
- Significant changes to Classy’s information security controls or processes
- Significant new security threats to Classy’s information systems, network resources, or data
- Information security best practices.

Employees must acknowledge, at least annually, that they have read and understood this Information Security Policy.

### 1.37 Risk Assessment

Classy requires a risk assessment be performed at least annually and after any major changes within the environment. The risk assessment process will examine the potential threats and vulnerabilities that could be associated with the environment and

the results of the risk assessment will be formally documented. In addition, if major changes were made within the environment, the risk assessments carried out for those changes will be provided along with any risk assessment procedures that are documented.

# Security Incident Response

## 1.38 Incident Response Policy

Classy must have a formal, documented security incident response plan. The plan must include:

- Roles, responsibilities, and communication strategies in the event of a security incident including notification of appropriate parties
- Specific incident response procedures
- Business recovery and continuity procedures
- Data back-up processes
- Legal requirements for reporting security incidents
- Coverage and responses for all critical Classy information systems
- Reference or inclusion of payment card brand incident response procedures
- Procedures for responding to alerts from intrusion detection (“IDS”), intrusion prevention (“IPS”), unauthorized wireless access points, and file integrity monitoring systems.

The security incident response plan must be tested annually and must designate specific personnel to be available on a 24/7/365 basis in order to respond promptly to information security alerts. The plan must be reviewed regularly and modified as necessary.

Classy employees who are responsible for responding to security incidents must receive regular and appropriate training in security incident response processes.

## 1.39 Non-Compliance Process

All staff covered by the scope of this policy are expected to adhere to it strictly. Any non-compliance to this policy must be reported to Information Security (security@classy.org) immediately. Failure to adhere to this policy may result in disciplinary action, including termination of employment.