



Information Security Practices & Procedures



Table of Contents

1. Purpose	4
2. Scope	4
3. Acceptable Use Policy	5
3.1. General Use of Edgio Systems	5
4. Roles & Responsibilities	7
4.1. Chief Information Security Officer	7
4.2. Information Security Department	7
4.3. System Administrators	8
4.4. Human Resources Department	9
4.5. End Users	9
5. Incident Response Plan	9
5.1. Identifying Security Issues	9
5.2. Reporting/Declaration Procedures	9
5.3. Typical Response	10
6. Required Policy & Document Reviews	12
6.1. Security Awareness Program	13
6.2. Security Review Policies & Procedures	13
6.3. Data and System Access	14
6.4. User Authentication	14
7. Anti-Virus Policy	15
8. Data Policy	15
8.1. Data Retention	15
8.2. Data Logging	16
9. Firewall/Security Group Admin	16
9.1. Change Process	16
9.2. Device Management Responsibilities	17
9.3. Allowed Services and Connection Paths	18
9.4. Personal Firewalls	18
10. Key Management Policy	19
11. Logging & Auditing Policy	19
11.1. Events Logged	19
11.2. Event Log Structure	19
11.3. Network Time Synchronization	20
11.4. Log Security	20
11.5. Review of Security Logs and Events	20
11.6. Review of Critical Security Control Systems	20
12. Physical Security Policy	21
12.1. Monitoring Physical Access to Sensitive Areas	21
12.2. Store, Inventory & Secure Media Containing Sensitive Data	22
12.3. Data Disposal Policy	23
13. Secure Data Transmission	23
13.1. Transmission Over Untrusted Networks	23
13.2. End User Messaging Technologies	23
14. Special Tech Use Policy	24
14.1. Approval	24
14.2. Authentication	24
14.3. Device Inventory	24
15. System Configuration Policy	25
15.1. Wi-Fi Access Point Vendor Defaults	25
15.2. System Configuration Standards and Deployment	25
15.3. System Purpose	25
15.4. System Security Configuration Process	25









15.5. Physical Servers/Windows Systems	26
15.6. "Critical Path" Systems	26
15.7. Edgio/Personal Computers	26
16. System & Apps Security Policy	26
16.1. Security Patches	26
16.2. Vulnerability Identification & Risk Assessment	26
17. Top 10 Vulnerabilities	30
18. Document Information	31
Version History	31

1. Purpose

This documentation aims to outline the various IT policies and procedures related to the acceptable use of Edgio computers and networks which all employees and contractors are expected to adhere to.

Edgio believes in maintaining an open work environment that relies on trust and transparency to achieve our shared business objectives in a secure manner. Through the development of a formal information security policy, including the acceptable use of Edgio computers and networks, Edgio aims to avoid compromising that culture of integrity by outlining basic measures to protect the Edgio and each other from harmful computer-related actions. Whether intentional or not, illegal or malicious activities cannot be tolerated under any circumstances.

The policy pertains to all Edgio-owned or operated:

-  computer equipment
-  operating systems
-  storage devices
-  internal/external applications
-  PDAs/smartphones
-  any other device with network access to the Internet or LAN

We also take the security of critical data and business-related assets very seriously. Therefore, management requires that all employees understand and comply with these policies. It is Edgio's intended purpose to protect client, employee, financial, protected third party and other corporate information from unauthorized disclosure, modification or destruction throughout the information lifecycle.

To accomplish this, Edgio has developed this set of IT Security Policies and Procedures in conjunction with a rigorous PCI DSS Compliance Assessment performed by a third-party Qualified Security Assessor. These policies offer direction to specific departments and staff members, and it is everyone's responsibility to uphold those policies that directly relate to their position at Edgio.

Policy Enforcement

Violations of this policy or related standards may lead to disciplinary action, up to and including termination. Any Edgio employee found to be in violation of these policies will face administrative discipline, which may involve a warning for minor violations or termination and legal action for serious offenders.

Brief Explanation of Payment Card Industry (PCI) Compliance

In September of 2006, the five biggest payment companies - VISA, American Express, Discover, JCB, and MasterCard - created the PCI Security Standards Council. The mutual goal was to create a single process that would enable companies to secure credit card data across all brands.



Together, they devised the Payment Card Industry Data Security Standard (PCI DSS) Program. This program enables merchants and service providers to safely store and process credit card information, whether they are using manual or computerized credit card processing solutions. E-commerce websites and POS devices that process information over the Internet are subject to the most demanding PCI assessments due to the heightened risk of online data interception.

2. Scope

These security compliance policies and procedures apply to all users of the computer systems and networks of Edgio, including but not limited to: all employees and associates of Edgio and its wholly-owned subsidiaries. They also apply to the activities of all Edgio personnel using or affecting Edgio's computer systems and networks. In addition, these policies and procedures apply to the activities of all third-party consultants, contractors, vendors and temporary employees using Edgio's computer systems and networks.

Any system component that is connected to the card-processing or data storage environment is in scope for PCI compliance. System components include servers, applications, employee PC's, and other network components.

Examples of everyday systems that are in scope for PCI compliance include:

-  Web/application servers that process credit card data.
-  Databases and PCs used to store credit card data.

- Firewalls or network devices used to transport cardholder traffic.
- Printers, fax machines, and other devices that may temporarily hold data.
- Support systems, such as syslog server, primarily used by system admins.

The policies and procedures contained in this documentation are intentionally broad in scope. The standards are specific and are regularly updated to keep pace with changes in business, technology and the business environment. Standards include details such as business process flows, roles and responsibilities, technical specifics and contract requirements.

3. Acceptable Use Policy

IMPORTANT! Any Edgio employee found to be in violation of these policies will face administrative discipline, which may involve a warning for minor violations or termination and legal action for serious offenders.

3.1. General Use of Edgio Systems

Be mindful of the data you create. Be advised that any data created on Edgio systems is the property of Edgio. Network Administrators strive to defend employee privacy whenever possible, but the intricacy and importance of data security means that privacy cannot be always guaranteed. The need to defend business interests trumps an employee's privacy, so be sure to use caution and sound judgment whenever creating or storing information on Edgio equipment.

All sensitive information, such as financial disclosures, customer credit card information, or internal earnings/stock reports, should be encrypted. Contact your supervisor to learn more about encrypting files.

Periodically, Edgio systems will be audited to ensure adherence to these policies. Be advised that an IT Security practitioner or Network Administrator may monitor network traffic at any time.

3.1.1. General Data and Information Security Policies

- Keep your network password a secret. Edgio systems remind users to update their password at regular 90-day intervals and users are responsible for keeping these passwords secure. Do not share accounts with other Edgio employees under any circumstances.
- Any data stored on Edgio systems must be defined as either confidential or non-confidential. Sensitive, or confidential, information may include financial disclosures, credit card numbers, bank statements, stock reports, proprietary information and any personally identifying customer or employee information. If you're unsure how a certain piece of information should be defined, ask your supervisor.
- Never leave your computer unprotected. Always remember to log off or lock your PC during breaks or when you are away from your desk. Additionally, all Edgio PCs have password-protected screensavers enabled to automatically turn on if a computer sits idle for 15 minutes. When a workstation is left unattended, confidential information might be viewed or downloaded.
- Confidential information should always be encrypted on your local machine. Never share unencrypted confidential information over email, IM, cloud services, public Wi-Fi or other unsecure communication channels. Even when encrypted, confidential information should only be shared over a secure connection or via an Edgio approved secure storage device.
- All employee-use laptops, whether Edgio or personally owned, must have firewalls installed and always operating. Exercise caution when transporting your laptop away from the office and make sure all local folders are encrypted.
- Avoid using your Edgio email addresses in public Internet forums, chat rooms or message boards unless it is directly related to Edgio business, and your supervisor is aware of the discourse. When checking your Edgio email, do not open attachments from non-Edgio email addresses or any unknown source/sender, as they may contain viruses or destructive malware.
- Virus-detecting software with a regularly updated virus database must be always installed and operational. The software should be set up to scan all email attachments and files downloaded from the Internet.

3.1.2. Normal Use vs. Inappropriate Use

For this policy, "normal use" is defined as any business-related activity that involves Edgio customers, partners, employees or the Edgio itself. Edgio equipment and systems should only be utilized for Edgio-specific purposes.

Utilizing Edgio computers and systems beyond normal business needs would be considered "inappropriate use" and a violation of Edgio policy. Edgio has developed this IT Security Policy documentation to inform employees of the risks and safeguards available to maintain data integrity and information security, which will serve to protect the Edgio's interests and reputation. Inappropriate use can expose Edgio to harmful viruses and

malware and may even allow malicious individuals to gain access to sensitive Edgio and/or customer information.

Examples of Inappropriate Use

Edgio has comprised a list of possible usages for Edgio equipment that should be avoided. Essentially, any activity that places Edgio systems, equipment, customers, employees or business information at risk of theft, unauthorized access, illegality or malicious intent is deemed inappropriate.

The following list is a basic guide on what is considered "inappropriate use" of Edgio resources. Certain employees may have a legitimate business need to use equipment and/or systems in a way that temporarily violates these IT Security Policies. Your supervisor must be aware of, and approve, any such actions that go against this policy. These actions should be limited in time and all efforts to avoid such actions should be explored prior.

- Under no circumstances should illegally obtained software be installed on Edgio machines. Edgio employees must always adhere to copyright law. If you do not own a license for software that you need for business purposes, speak with your supervisor. Additionally, duplicating copyrighted images or other media for Edgio purposes is strictly forbidden.
- Employees must obtain explicit approval before accessing Edgio networks and Wi-Fi with personal devices/smartphones/tablets/laptops.
- Avoid sharing, copying or otherwise distributing files obtained from websites or personal email on Edgio systems. This may introduce malware, viruses and Trojans that would otherwise be detected by Edgio anti-virus software.
- Never share your Edgio network name or password, even with family and friends.
- Never use Edgio systems to harass co-workers or create a hostile work environment.
- Never use Edgio email or systems to promote fraudulent claims about Edgio services or respond to a negative public comment. Be careful what you post and always double-check your email communications before sending.
- Do not allow unauthorized users to access Edgio systems using your credentials. Do not give access to contractors, temporary workers or interns without approval from your supervisor.
- The IT department is responsible for conducting regular security scans of ports and analyzing network traffic flow. Do not engage yourself in any of these activities unless directed by the IT Coordinator.
- Do not attempt to access Edgio systems in any other manner besides using your own unique username and secure password. Sharing credentials with other employees is prohibited.
- Do not attempt to access Edgio networks from a remote location without prior written approval from your supervisor and proper security measures in place.
- Never provide personally identifying information about co-workers over the phone, email or on public websites.
- Never distribute Edgio's employee roster or work schedule.
- Do not use Edgio email to send or forward "spam" or junk email, including unsolicited advertisements, promotions or any material not requested by the recipient. This may include money-making schemes and inappropriate jokes/photos.
- Never use your Edgio email when posting non-business-related material to public website forums.
- Email signatures should contain accurate contact information with official Edgio phone numbers, addresses and titles included.

These guidelines are intended to avoid, among other things, a data breach of Edgio systems. A data security breach may include theft of information, planting of malware, gaining access to privileged information and using Edgio systems to launch more sophisticated attacks. Employees may inadvertently cause a security breach by giving out usernames/passwords, allowing unauthorized access to servers or performing a task that falls outside of normal business operations.

As part of Edgio's pursuit of overall IT Security Awareness, reminders and tips on good conduct will be regularly emailed to all employees. The IT department will inform employees about critical patches and updates to Edgio software. Complying with these official Edgio security requests is mandatory for all employees.

4. Roles & Responsibilities

4.1. Chief Information Security Officer

The responsibilities of Edgio's Chief Information Security Officer (CISO) include enforcing these policies and procedures and working closely with Edgio executives and business unit managers to identify additional areas of concern. Once identified, the CISO works with Edgio's management to coordinate the repairs or changes as needed.

Further responsibilities of the CISO include:

- Performing an annual review of the Information Security policies and procedures document, which helps to maintain the accuracy of the document and addresses any new or perceived threats.
- Ensuring that all information security initiatives are aligned with Edgio's regulatory compliance, governance, and security directives.
- Performing an annual risk assessment that will identify new threats or vulnerabilities.
- Overseeing the analysis of any security alerts and disseminating information and instructions to appropriate Edgio personnel.
- Executing the assignment of user account and authentication management to authorized information security personnel.
- Ensuring all third-party vendors that store or handle Edgio's data assets is contractually obligated to comply with PCI DSS requirements. In addition, any connections to the third-party vendors must be managed per the PCI DSS requirements.
- Ensure Executive Management has assigned overall accountability for maintaining the entity's PCI DSS compliance all accountability for maintaining PCI DSS compliance.
- Defining a PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management.

4.2. Information Security Department

To successfully secure Edgio's information systems, all departments must adhere to a consistent vision for information security. This challenge is met through the creation of an Information Security department, which works with managers of each department to develop the standards, which will protect Edgio assets.

The three main areas of focus for an Information Security department are security awareness, education, and security planning.

More specific responsibilities include:

- Reviewing the policies and procedures annually, then creating and/or updating this documentation as necessary.
- Restricting access to sensitive areas.
- Distributing and updating incident response plans and escalation procedures.
- Implementing/coordinating Information Security policies when and where appropriate.
- Monitoring for security alerts, and informing Edgio management and other security personnel.
- Reviewing security logs on a daily basis and reporting any discrepancies.

4.2.1. User Access Management

The Information Security department approves user access based on the roles of each user. Any requests for network access must contain an approval (either written or in electronic form) from the Information Security department.

Guided by a specific business unit's management, the Information Security department will determine a user's access level based on their responsibilities and needs.

To determine that all access privileges are up-to-date and accurate, the Information Security department will perform a bi-annual audit of all network authorizations by validating access rights for sample user populations. If access cannot be determined based on a defined business role, additional approvals must be collected by the Information Security department before access is authorized. Contractor accounts, or any other extension authorizations, must also go through the Information Security department.

4.2.2. Emergency IDs

If access must be granted to correct an issue or resolve some other network problem, the Information Security department may issue an Emergency ID. That process goes as follows:

1. An emergency ID request must be made through the Information Security department, who will then notify all relevant departments and the proper System Administrator.
2. Once work has been completed, the user must notify the Information Security department so they can disable the ID.
3. To avoid delaying access, an Emergency ID Request Form must be completed as soon as possible and filed by the Information Security department.

4.3. System Administrators

Representing the direct link between Edgio policies and the network, Edgio System Administrators are vital to the upkeep of information security.

Their primary responsibilities include:

- Restricting physical access to wireless hotspots, network jacks, handheld devices and other network gateways.
- Managing user accounts and the authentication process.
- Applying Edgio policies and procedures when and where appropriate.
- Assisting the Information Security department in analyzing and controlling access to Edgio data.

Additional areas of responsibility include:

- Any requests for access must clearly state the role of the user and how that role is associated to the desired level of access. Any new accounts that are created by mirroring an existing user account are required to be audited against the request or roles determined to be appropriate for access.
- A user's identity must be verified before any password resets are allowed by mail, telephone, or email.
- When the System Administrator receives notice that access has been revoked, that access should immediately be disabled. To ensure that access for a terminated employee is revoked right away, written procedures should be in place. The System Administrator should suspend any users who are on an extended leave of absence or long-term disability. This employee status information can be validated by utilizing Edgio's Human Resources systems.
- After 60 days of inactivity, a User ID should be disabled. After 90 days of inactivity, the User ID should be removed from the system. Certain IDs, such as NT Admin or root, are exempt from this policy but require the System Administrator to file a written waiver with the Information Security department. The waiver will include documentation detailing compensating controls around access to the accounts in question.
- Audit logs must be enabled to record user activities (including administration). These audit logs must be stored for a minimum of 90 days for immediate access, then archived for up to one year (365 days).
- The user must change any passwords set up by the System Administrator during their first login. System Administrator passwords must also be unique and follow the password policy.
- Prior to performing a password reset, the System Administrator must validate the identity of the requester.
- Any authorized contractor accounts should be set to expire at the end of the contract. Any necessary extensions may be requested through the Information Security department. These temporary accounts should be monitored carefully.
- Accounts for terminated employees and users who no longer have a need for their level of access should immediately be disabled.
- When Edgio does business with a remote vendor, their access to the system should only be authorized when needed to perform remote functions.
- Ensure authentication for access to all systems, with a focus on access to databases containing cardholder or other highly sensitive data.

4.4. Human Resources Department

The Human Resources department plays an important role in Edgio's information security. This is due to their direct relationship with employees (both current and former).

As related to information security, the following duties are the responsibility of Human Resources:

- Distribute the Employee Handbook to all Edgio employees, with a link to this documentation.
- Work with the Information Security department to formulate sanctions and other disciplinary actions involving violations of security policies.
- Perform background checks on those employees with access to network systems and critical data. Checks must include background, criminal, pre-employment, credit history and references.
- Coordinate employee terminations with personnel responsible for Access Management.

4.5. End Users

All users of Edgio resources, computers and network systems must understand the importance of information security. In doing so, they will recognize their own crucial role in safeguarding critical data and maintaining Edgio systems.

These specific responsibilities apply to all Edgio information system users:

- Assist Edgio in meeting its business goals by understanding that their actions have real consequences. Users must act accordingly, especially when it pertains to information security policy.
- Avoid distributing classified or sensitive information.
- Maintain an understanding of current information security policies.

5. Incident Response Plan

5.1. Identifying Security Issues

All Edgio employees share the responsibility of detecting and reporting security incidents!

It is mandatory for all employees to assist the incident response procedures by managing their personal area of responsibility. The types of security incidents that an employee might likely encounter in their daily work routine includes:

- Security event notifications (e.g. natural disaster alerts, file integrity alerts, intrusion detection alarms, physical security alarms)
- Fraud (e.g. inaccurate database information, inaccurate logs/records)
- Theft or unauthorized access (e.g. surveillance/CCTV evidence of a break-in, missing items, unauthorized logins, broken locks)
- Unusual system behavior (e.g. unscheduled system reboots, abnormal errors in system log files/terminals)

Every employee should possess a working knowledge of these possible incident identifiers, as well as the appropriate team member to notify. All employees must report incidents per the guidelines in 14.3 (Reporting and Incident Declaration Procedures), unless they are otherwise occupied with a separate aspect of the incident response plan.

5.2. Reporting/Declaration Procedures

When an employee reports a possible incident, the Information Security department should be notified – especially if it deals with a critical component of Edgio's business environment. The Information Security department can best assess whether a reported issue is really a security incident or not.

To maintain the integrity of both the incident investigation and recovery process, Information Security department personnel should be the sole investigating and remediating agent. However, when a possible security incident is noticed the employee should do the following as soon as possible:

- If the possible security incident involves a Edgio computer system:
- DO NOT alter or modify the computer system. The computer should be left powered on, with all software/programs left running.
- DO NOT power down or restart the computer.

- IMMEDIATELY change security groups to block all network ingress and egress.
- Report the Incident:
- IMMEDIATELY contact the Information Security department and report the incident.
- DO NOT communicate this incident to other employees, except for supervisors and the Information Security department.
- DO NOT contact the police. If necessary, communication with law enforcement will be coordinated by the Information Security department.
- While waiting for the investigation to begin, employees should document any pertinent information that will aid in responding to the matter. The documentation should include date, time, and the nature of the incident.

Severity Classification

After a possible security incident is reported, the Information Security Department must determine if the incident requires a formal response.

For incidents that do not require a formal response, the Information Security Department will notify the appropriate IT personnel who will perform any necessary support services that may be necessary.

The Information Security Department should determine the appropriate response based on the following:

Classification	Description
Level 1	Corresponds with one instance of potentially hazardous activity.
Level 2	Corresponds with either a second Level 1 attack, or ONE instance of an obvious attempt to access unauthorized information/systems.
Level 3	This level corresponds with either a second Level 2 attack or an actual security breach.

NOTE: A Level 1-type attack that focuses on systems storing sensitive or confidential information should be classified as Level 2.

5.3. Typical Response

The stages of a typical response are:

1. Identification
2. Severity classification
3. Containment
4. Eradication
5. Recovery
6. Root Cause Analysis

Finally, an overall improvement of security controls should transpire because of the findings. Once an incident has been identified and classified, the Information Security department will be responsible to take the following actions:

5.3.1. Level 1

Contain the Incident and Monitor for Changes

1. Whenever possible, document the user, IP address and domain of intruder.
2. Block the intruder's access via approved technology controls.
3. Monitor for future breach attempts originating from the documented user or IP address.

5.3.2. Level 2

Contain the Incident, Monitor for Changes and Warn Others

1. Document and securely store any information associated with the incident.
2. Block the intruder's access via approved technology controls.

3. Attempt to track down the connection's origin.
4. If possible, contact the ISP and gather information regarding the incident or suspected intruder.
5. Perform research as to the possible ramifications surrounding the chosen method of attack. If applicable, re-evaluate and re-classify the severity level rating (adhering to the Level 3 guidelines for containment, eradication and recovery).

Once the source is identified, notify the malicious user that Edgio has knowledge of their activities. Warn them of future recriminations if another attempt is ever made. If a Edgio employee is found to be the culprit, management should work with Human Resources to appropriately address the Acceptable Use violation.

5.3.3. Level 3

Contain the Incident, Eradicate the Issue, Recover & Perform Root Cause Analysis

1. For any incident involving cardholder data or systems, a notification must be issued to the Acquirer and any related card associations.
2. Contain the incident/intruder by unplugging the network cables, applying restrictive ACLs, deactivating the user's ID, isolating the switch port, or terminating the user's session and ability to change passwords.
3. Document and securely store any information associated with the incident via offline methods. If necessary, the Information Security Department will work with legal and Edgio management to employ forensic specialists.
4. Continually update management on the progress of each step.
5. Delete or eliminate the intruder's access path and any associated vulnerabilities.
6. Perform research to determine the connection's origin.
7. If possible, contact the ISP and gather information regarding the incident or suspected intruder.
8. Perform research as to the possible ramifications surrounding the chosen method of attack.

5.3.4. Special Response to Credit Card Companies

The Information Security Department must follow this procedure for any security incident that involves a potential compromise of credit card information or personal cardholder data.

1. The Information Security Department must first contain and/or eliminate the threat and avoid further exposure. A thorough investigation into the security breach must be performed within 24 hours of the incident. These steps should be taken to assist the investigation:
 - a. Document all steps/actions taken.
 - b. During the transfer of any materials or information related to the investigation, employees must utilize chain of custody techniques.
 - c. Do not log on to the affected systems, change any passwords or otherwise access/alter the systems. Do not log on as ROOT.
 - d. Do not turn the affected system off. It is important to isolate any compromised systems from the network. Isolation can be achieved by unplugging the network cable, deactivating switch ports or isolating the system to a contained environment (e.g., isolated VLAN). Disaster Recovery/Business Continuity procedures should be used to recover any lost or disabled business processes.
 - e. Archive or store all logs and other electronic evidence.
 - f. Change the wireless network SSID on the AP and other non-compromised machines (if applicable).
 - g. Maintain vigilant to any additional threats and monitor all cardholder information systems.
2. Alert all relevant parties. The following should be notified:
 - a. U.S. Secret Service (if VISA payment data has been compromised).
 - b. Local FBI Office.
 - c. Merchant Bank.
 - d. If not already involved, the Incident Response and Forensic Teams.

3. Specific cards have additional procedures. Follow these procedures for any cards that Edgio accepts:

VISA

Within 10 business days, the VISA Fraud Control Group must be provided with all the compromised VISA accounts. The VISA Fraud Control Group will advise on how to securely transmit any account numbers. For assistance, call (650) 432-2978. VISA will distribute the compromised account details to issuers and will ensure the continued confidentiality of non-public and entity information.

Mastercard

Contact Edgio's merchant bank to obtain details on how to handle a compromise involving Mastercard cardholder data. The merchant bank can assist with contacting Mastercard at (636) 722-4100.

American Express

Contact Edgio's American Express representative, or call (800) 528-4800.

Discover Card

Contact Edgio's Discover Card representative, or call (800) 347-3083.

JCB

Contact Edgio's JCB representative, or call (213) 896-3718.

5.3.5. Root Cause Analysis and Lessons Learned

To determine the root cause of the security incident, the Information Security Department and all affected departments/employees will meet within one week of the incident to review results of the investigation. During this review, the effectiveness of the Incident Response Plan will be evaluated. Additionally, security controls will be reviewed to determine their effectiveness. Updates to the Incident Response Plan, security controls and other policies and procedures will be made accordingly.

5.3.6. Plan Testing and Training

On an annual basis, the current plan will be tested by means of a "mock incident." The Information Security Department will facilitate and plan the incident at their discretion. All procedures outlined above must be followed, including the follow-up session. This test will involve all Edgio employees who have an active role in the Incident Response Plan.

5.3.7. Automated Security System Notifications

Automated intrusion detection systems, such as detection sensors and file integrity monitoring (FIM) systems, should be configured to automatically alert the Information Security Department of any potential threats. FIM solutions should be used to protect logs as well as any system-level objects. System-level objects are anything on a system component that is required for its operation, including but not limited to application executable and configuration files, system configuration files, static and shared libraries and DLLs, system executables, device drivers and device configuration files and added third-party components.

One Information Security Department Engineer must be "on-call" 24 hours a day to respond and initiate the Incident Response Plan.

6. Required Policy & Document Reviews

The Information Security Department shall be responsible for maintaining the information security policy and ensuring that all personnel and relevant third parties receive a copy.

All users must read and understand Edgio's Information Security Policies and Procedures. By signing the Security Acknowledgement and Acceptable Use Policy, the user is declaring an understanding of policy prior to accessing Edgio's network systems.

On an annual basis, the Chief Security Officer must ensure Edgio data assets are sufficiently protected by coordinating a formal risk assessment. This assessment will identify any existing or new vulnerabilities. The information security policy will be updated as necessary to reflect any findings from the risk assessment.

6.1. Security Awareness Program

The Edgio Chief Security Officer will oversee, and the Information Security Department will execute security awareness training for all Edgio personnel. Initial training must be provided for personnel upon hire and periodic refresher training must occur annually at a minimum. The method of delivery as well as the topics can vary depending upon the audience. The Information Security Department will determine and approve training methods and topics. Where training is performed in a group setting, a sign-in sheet will be circulated for attendees to record their attendance. The Human Resources department will maintain a record of sign-in sheets.

6.1.1. Employee Background Checks

New hire candidates for positions requiring access to sensitive systems and applications involving credit card data, a background check will be ordered by the Human Resources department.

6.1.2. Third-Party Information Sharing - Due Care & Due Diligence






The Information Security Department shall maintain a list of service providers with whom Edgio shares credit card data. Edgio must exercise due care in maintaining written agreements between Edgio and any service providers. Such agreements must include language where the service provider acknowledges their responsibility to secure credit card data where they are involved in the storing, processing and/or transmitting of this data.

In addition, Edgio must exercise due diligence prior to engaging service providers. Service providers should be vetted thoroughly prior to establishing a formal relationship. Part of this process should include checking references and professional accreditations. Preference will be given to service providers who have undergone and passed the rigors of a PCI DSS Level One Audit. Once a service provider is engaged, Edgio must monitor the service providers' PCI DSS compliance status annually. This process will require Edgio to request a copy of the service providers' Attestation of Compliance (AOC) on an annual basis.

Edgio will also maintain a clear list of responsibilities visa-vis PCI for it's customers, so that PCI coverages is properly maintained.


6.2. Security Review Policies & Procedures

All applicable policies, procedures, and processes should be reviewed at least quarterly to confirm that personnel are following Edgio security policies and operating procedures. These reviews must encompass the following processes:

-  Daily log reviews
-  Firewall rule/security group reviews
-  Applying configuration standards to new systems
-  Responding to security alerts
-  Change management processes

6.2.1. Maintenance of Quarterly Review Documentation Process

In addition to the above, service providers such as Edgio must maintain documentation of each quarterly review, and include:

-  Documented results of the reviews
-  Review/sign off of results by personnel assigned responsibility for the PCI DSS compliance program

6.2.2. Critical PCI Documents

Document/Policy	Description
Document Review Management Log	Lists policy and other documents/materials which are required by PCI to review. It should contain when we last reviewed it, when and by whom, and whether changes were made or not.
Firewall Rules Review Log	Lists our current firewall rules/security groups in production, and notates any differences along with remediations.

6.2.3. Access Control Policy

6.3. Data and System Access

The Edgio Platform does not store data. As such, it does not have any data classification systems. All customer data in transit through the Edgio Platform is treated as sensitive and confidential.

Edgio systems must use an automated access control mechanism. Access controls must be configured and operational to track all access to data – including the user's identity, time and date, and a listing of the accessed data. This system of controls protects sensitive data and ensures that the information is not improperly distributed, copied, modified, or deleted.

Access to network systems and data must be limited to those employees who have been properly authorized. Each user will be authorized to view a certain classification level. All access must be configured to authorize only the data each user needs for their specific position or business role. Every user must be authorized to access Edgio's systems. Authorization pertains to the user's business role and will only be authorized when necessary to fulfill said role.

System access requires that roles be clearly defined in the Roles List, and that the Edgio Authorization Form be completed.

6.3.1. Required Login Notice

Any network or computer resource that can display a sign-in message must display the following text at some point during the login process:

This system is for the use of authorized users only. Usage of this system may be monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

6.4. User Authentication

Each authorized user will be given a unique account ID. The user will create a secret password, and all Edgio systems must authenticate via passwords.

6.4.1. Remote Access Authentication Requirements

Edgio employees or third-party vendors must incorporate multi-factor authentication for all non-console access into the cardholder data environment (CDE) for personnel with administrative access.

In addition, multi-factor authentication is required for all remote network access (both user and administrator and including third party access for support or maintenance) originating from outside the entity's network.

Two-factor authentication employs two of the three following authentication methods:

- Something you know (example: password or passphrase)
- Something you have (example: soft or hard tokens, smart card or valid and unique digital certificate installed on user's workstation)
- Something you are (example: biometric)

It is not acceptable to employ one of these methods twice. For example, requiring a user to enter two different passwords does not constitute two-factor authentication.

Authorized Edgio personnel will actively manage those IDs used by third-party vendors as follows:

- Vendor access will be enabled only during the time needed and disabled when not in use.
- Vendor access will be intently monitored when in use by all appropriate means.

6.4.2. Password Policy

User-level access must include authentication measures, such as a password. Non-authenticated user IDs, shared IDs, and group IDs are not permitted. Each Edgio system must employ an automated access control process. This process will:

- Expire passwords after a period of 90 days.
- Authenticate every account (meaning all users, systems, and applications) with a password.
- Require passwords of at least 8 characters, which include a combination of upper, lower, numerical, and special character cases
- Cannot contain user ID
- Must be different than previous 4 passwords.
- Identify every user by their unique account name.

- Require that a user account will be locked out of the system after 6 failed attempts to connect.
- For laptops & AWS: The account will remain locked until a Systems Administrator unlocks it.
- For customer applications: The account can be unlocked by resetting password via email or by answering security questions.
- Require that the system disconnect a user after an idle time of 15 minutes.
- User IDs that are inactive for 90 days are automatically locked.

Individuals granted network access for the first time and individuals requesting a password reset must be granted a unique password that must be changed after first use. Furthermore, for all non-face-to-face password-reset requests, the System Administrator must verify the user's identity.

Any Edgio employees or vendors that have network access must have that access immediately revoked once their relationship with Edgio is severed for whatever reason. Vendor user accounts should only be enabled when needed. Furthermore, vendor access (both remote access and local access) must be monitored.

7. Anti-Virus Policy

All Edgio computer assets, including file servers and email servers managed by employees or third parties, which run the Microsoft Windows OS must comply with this policy.

Information Security department must approve any policy exemption in writing.

The Information Security department is responsible for approving anti-virus/anti-spyware software and configuring it for each system. Users must not be able to disable or otherwise configure the software. The approved software must perform real-time scans and log all anti-virus alerts with routing to a central logging solution. All anti-virus software should be configured to run daily virus signature updates.

If a virus is detected during a real-time scan, the Information Security department must be alerted at the same time.

Based on the Incident Response Plan, the Information Security department will determine how best to resolve the virus alert.

All anti-virus software logs will be stored/archived in accordance with Edgio logging and auditing policies and procedures. Logs must be retained for at least 365 days, with 90 days immediately available for analysis. Logs must record all information necessary to reconstruct a security event. Logs should include:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component or resource

Specific security guidelines for Edgio laptops should be followed.

8. Data Policy

8.1. Data Retention

IMPORTANT: Edgio systems do not store any credit card data.

Information Security department must provide written approval for any exemptions to this policy.

All data assets stored on Edgio systems that are classified as sensitive or confidential must adhere to this policy. For credit card data, only the primary account number (PAN), cardholder name, expiration code and service code may be stored. In addition, an encrypted PAN is deemed to be PAN data that must adhere to this policy.

The data creator or authorized manager must establish a specific retention timeframe for any sensitive or confidential data stored on Edgio systems. This information may be retained until legal, regulatory and business requirements have been met.

Generally speaking, single use cardholder data may be retained for up to 120 days. However, cardholder data used for recurring transactions may be retained for as long as the customer's account remains with Edgio. If the customer's account is deleted, that cardholder data must also be deleted/purged from the system within 120 days using approved disposal methods.

Specific cardholder authorization details, including PIN numbers and CVV2, will be retained only until the current transaction is completed. Retention of this data post-authorization is not allowed under any circumstance.

8.1.1. Displaying Credit Card Primary Account Number (PAN)





No Edgio employees shall have visibility to the full PAN except for those who have a legitimate business need to see the full PAN. Displaying full PAN on computer screens, receipts, faxes, or any kind of hard copy media is against Edgio policy. A maximum of the first six and last four digits of the PAN may be displayed. All other digits must be masked. This policy is intended to protect credit card numbers as they are displayed and should not be confused with stricter requirements relating to storage of credit card numbers, which must utilize strong encryption, hashing or truncation.

Any application used by Edgio that displays credit card information must be configured to hide or mask that sensitive or confidential data (if possible). If the purpose of the application involves displaying the full credit card number, or other personal data, approval for its use must be given by the Information Security department. In all cases, this type of application must be limited to the fewest possible number of required users.

8.1.2. Encrypting Stored Cardholder Data

This encryption policy applies to all applicable Edgio computer systems and primary as well as secondary storage locations, whether managed internally or by third party vendors. Examples of primary storage locations include but may not be limited to databases and flat files such as spreadsheets. Examples of secondary storage locations include but may not be limited to backup media such as USB thumb drives or tapes, and audit logs such as history, error, debugging, or transaction logs. Encryption must be employed for any stored credit card primary account numbers (PANs) and the entire PAN shall be encrypted. Card validation codes (CVV numbers) for card-not-present transactions and PIN blocks must never be stored post- authorization under any circumstances.

One of the following methods must be employed to protect the PAN anywhere it is stored:



-  Strong cryptography with associated key management processes and procedures
-  Truncation
-  Strong one-way hash functions with salts
-  Edgio tokens and securely stored pads

8.2. Data Logging

Edgio systems must never log HTTP(S) POST or other form data, cookie data or any other customer data in any form.

9. Firewall/Security Group Admin

The following are in-scope for this policy:

-  Physical routers or firewalls
-  Amazon Web Services (AWS) security groups or network access control lists

Exemptions may only be authorized with written approval from Edgio management or an approved Security Officer.

9.1. Change Process

Firewalls are categorized as production systems as they support Edgio information systems. Any and all changes to the firewall must be approved in advance by the Information Security department. The changes must be thoroughly tested (following production standards) as outlined in the Change Control Policy.

Examples of changes include:

- Upgrades or patches to the firewall system
- Modifications to any firewall software or system
- Additions, deletions, or modifications of any firewall rule
- Additions, deletions, or modifications of any AWS security group, or network access control list

9.1.1. Change Approval Process

1. Verify that the proposed change will not materially change the Network Points of Entry diagram. If there will be a change, file a ticket in Clickup and update related documentation.
2. Perform the change(s) as proposed.
3. Automation pulls data from API and checks differences into source control.

9.2. Device Management Responsibilities

The team responsible for managing Edgio firewalls, routers, AWS security groups and AWS network access control lists will be comprised of the Information Security department and key non-IT staff members.

Roles and Responsibilities

Edgio will maintain a clear list of roles and responsibilities that will be updated on a regular basis. Specifically, the Information Security department is responsible for the following related to firewall/security rule management:

- Ensures that any changes to firewall hardware, software, or security rules are authorized by the Information Security department and follow appropriate change control policies.
- Ensures that all router configuration files are synchronized and secure.
- Uses Permitted Network Services and Protocols to document any firewall security rule changes.
- Mitigates security events by coordinating a sufficient response plan with the Information Security department.
- Reviews and updates network diagrams after any changes are made.
- The diagrams must accurately describe firewalls, access control systems, anti-virus software, IDS/IPS, and any other connection to confidential or sensitive information.
- Reports any discovered vulnerabilities or security events to the Information Security department.
- On a daily basis, monitors all logs that capture and report security events.
- Provides the Networks Operation Center read-only access to logs related to security events and the performance of critical systems.
- Keeps track/monitors system alerts related to critical systems.
- These alerts might include system reboots, firewall daemon failing, etc.
- In the event of a security system failure, alerts the appropriate department.
- Assures Edgio management that the security rules applying to firewalls are sufficient to protect assets from unauthorized access.
- Assures Edgio management that the security rules applying to firewalls are sufficient to prevent internal security threats from exiting the network.
- Mitigates security risks by developing an appropriate response plan with the System Administrator.
- At least every six months, ensures the network diagrams are up to date.
- Identifies internal or external threats by actively monitoring firewall security events.
- Performs a thorough review of any proposed firewall and router security rule change, and ensure they meet policy compliance before allowing the proposal to continue through the change management process.
- Ensures the proper documentation of all services allowed through the firewall.
- For risky protocols, performs or approve a risk assessment and ensure the protocol has a specific business need.

9.3. Allowed Services and Connection Paths

Every path and service that is not specifically approved by this policy must be blocked.

All inbound Internet traffic must use a network segmented by a firewall or security group. This segmented zone is known as the DMZ. This inbound traffic must be limited to only those ports deemed necessary for Edgio business. With the exception of the DMZ, perimeter routers should never be configured to include a route to internal address space.

- Inbound/outbound rules are set using AWS security groups.
- The application servers reside on the private (or internal) subnet.

9.3.1. Inbound Connections

AWS security groups prevent all inbound connections to the private subnet.

9.3.2. Outbound Connections

AWS security groups limit outbound connections from the private subnet. There is one exception, with a compensating control:

The app user on the application servers is allowed to make outbound connections over HTTP/HTTPS. This is necessary because our proxy has the feature of being able to 'pass through' and modify any HTTP component, on any domain.

All firewall and router configuration files must be secured to prevent unauthorized tampering. In addition, the startup configuration files must be synchronized with the secure settings of the running configuration files in order to prevent weaker rules from running in the event that one of these devices restarts.

Network Address Translation (NAT) must be used to hide private subnet IP addresses.

Perimeter devices must be equipped with anti-spoofing technologies. These devices will reject all traffic that includes:

- A destination IP address matching RFC 1918 address space.
- A source IP address matching RFC 1918 address space.
- A source IP address matching any Edgio-owned address space.

Internal production systems with outbound traffic must also use the DMZ network. This type of traffic should also be limited to only required protocols and services.

Any Edgio databases must be stored on a private subnet that is segmented from the DMZ network.

All inbound connections to internal production payment systems, and originating from Edgio wireless networks, are forbidden.

Internet and wireless segmentation must employ a stateful packet inspection firewall. This will allow only established connections in or out of the network.

For cardholder environment segmentation, VLANs with compliant ACLs may be used – so long as the VLAN switch is PCI compliant and hardened to deter switch exploits such as ARP cache floods. VLANs must be established according to the same requirements that apply to firewalls.

9.4. Personal Firewalls

Personal firewall software must be installed and activated on any Internet-connected mobile device or computer that also accesses the Edgio network. This software must have a non-user alterable configuration as deemed suitable by the Information Security department.

All mobile devices or computers with administrative access to the CDE and which are used to access Edgio's production network are required to have personal firewall software. The firewall must not be configurable without administrator access, as is the default behavior on Mac OS X. Ubuntu desktops will run UFW.

10. Key Management Policy

Encryption keys must be generated, accessed and stored in a secure manner. In order to generate a strong key, a random or pseudo-random number generation algorithm must be used. The minimum length requirements for the encryption keys are 128 bits. Examples of acceptable algorithms are as follows:

- • AES: 256 bits
- • RSA: 2048 bits

Always follow the latest vendor recommendation(s) for encryption types and algorithms.

Any key used to either encrypt or decrypt cardholder data must be stored separately from general user access.

- Key components may only be accessed by authorized key custodians.
- Key generation must be done through our automated systems.

Encryption key component access will only be given to key custodians with a job duty that requires access. The Information Security department will be responsible for granting access by utilizing an 'Authorization Request Form'. Users who have been granted access must complete and sign an 'Encryption Key Custodianship Form'. By signing the form, the user recognizes their responsibilities as a key custodian.

Human Resources will maintain a copy of this form in the user's employee records.

Only those authorized key custodians will be allowed to retrieve the key components from their secure location and distribute keys. Key custodians must track and log their activities within an 'Encryption Key Management Log'. Before being returned to secure storage, the custodian must place the encryption keys in secure packaging.

During an encryption key change process, the key custodian generates a new key, decrypts the current production data and re-encrypts the sensitive data with the new encryption key.

On an annual basis, or whenever conditions warrant a change in key integrity, the encryption keys must be changed. Conditions for a key change include:

- Annual Rotation: Keys are to be changed once per year (minimum).
- Suspicious Activity: Keys are to be changed if any activity related to the key process raises concern or is otherwise deemed suspicious.
- Resource Change: Keys are to be changed if a key supervisor's employment ends or a key custodian accepts a position within Edgio that does not involve the key encryption process.
- Technical Requirement: Keys are to be changed if a technical issue arises that questions the durability or security of a key (corruption or instability).

To dispose of an unwanted encryption key, key custodians must follow approved Edgio methods for secure data disposal.

11. Logging & Auditing Policy

11.1. Events Logged

To reconstruct the following events, all system components must have an automated audit trail implemented.

- Invalid logical access attempts.
- All user access to cardholder data.
- Creation or deletion of system-level objects.
- All administrative actions utilizing user IDs with access above-and-beyond that of a general user (e.g., root, oracle, Admin group privilege).
- Access or initialization of audit log files.
- Any user or admin authentication attempts (either valid or invalid).

11.2. Event Log Structure

All system access event logs must contain the following minimum information:

- Name of the affected data, system component or resource.
- User ID.
- Origination location of event.
- Type of event.
- Date and Time that event occurred.
- Result of the event.

11.3. Network Time Synchronization

All Edgio production systems must be configured to use the Amazon Time Sync service for time synchronization purposes (NTP).

11.4. Log Security

All event logs must be securely stored in a centralized location or on a storage device that is protected from unauthorized access. The logs will only be accessed and viewed on a "need to know" basis. Wireless logs must be copied onto a log server housed on the internal LAN. Furthermore, the Information Security department must establish a file integrity monitoring (FIM) system that will alert personnel in the event either unauthorized access to logs or modification of logs occurs.

Logs must be retained for a minimum of one year with three months (90 days) immediately available for analysis. If logs are archived on removable media and stored at an offsite location, attention should be paid to ensure that the most recent three months are kept onsite so that they can be readily analyzed should a security event occur.

11.5. Review of Security Logs and Events

The following items are to be reviewed by authorized personnel daily in order to identify any suspicious activities or irregularities:

- All security events
- Logs of all systems that store, process, or transmit cardholder data or sensitive authentication data
- Logs of all critical system components
- Logs of all servers and system components that perform security functions

In addition, authorized personnel will periodically review logs of all other system components and follow up on any suspicious activity or irregularities identified during the review process.

Log retention should be defined in the policy. Procedures for retaining audit logs for at least one year (365 days) with a minimum of three months (90 days) immediately available for analysis.

11.6. Review of Critical Security Control Systems

Edgio has established processes in place that aid in ensuring the timely detection and reporting of failures of critical security systems. These include, but are not limited to, the following:

- Firewalls
- IDS/IPS
- FIM
- Anti-virus
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Segmentation controls

Edgio has established processes in place for responding to a security control failure. These include, but are not limited to, that include the following:

- Restoring security functions
- Identifying and documenting the duration (date and time start to end) of the security failure
- Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause
- Identifying and addressing any security issues that arose during the failure
- Performing a risk assessment to determine whether further actions are required because of the security failure
- Implementing controls to prevent cause of failure from reoccurring
- Resuming monitoring of security controls

When documenting security control failures, Edgio personnel will make sure to identify the root cause of the failure, the duration of the security failure (date and time start and end), and will provide details of the remediation required to address the root cause.

12. Physical Security Policy

Amazon Web Services (AWS) maintains physical security of all Edgio's production systems. These items are listed in the event Edgio ever decides to maintain systems outside of AWS.

12.1. Monitoring Physical Access to Sensitive Areas

Physical access controls must be established to protect hard copy, printed materials and electronic media used to store any Edgio information.

- Access to physical network jacks, wireless access points and handheld devices must be restricted.
- Sensitive areas must be monitored by security cameras. The data collected must be stored for at least 3 months.
- Relevant facility controls must monitor and/or restrict access to any systems that store or process Edgio information.

12.1.1. Handling Visitors & ID Badges

It is mandatory for all Edgio employees, contractors and visitors to clearly always display their ID badges. Employees should be watchful for unknown persons or fellow employees not displaying an ID badge.

The badge distribution area should be kept in a physically secure environment and monitored by the Information Security department.

The ID badge area, Edgio data center and other restricted areas must display a visitor log. Anyone accessing these areas must complete an entry in the log, and include:

- Name
- Date
- Edgio or department
- Name of Edgio employee who authorized the access

This visitor log information must be stored for at least 3 months.

Upon facility entry and completion of the visitor log, the receptionist will provide visitors with an ID badge containing no assigned access privileges. This type of ID badge is noticeably different than a regular employee ID badge. The receptionist will issue an expiration date of no longer than one day for each visitor ID badge.

For access to certain areas, employees may request a visitor badge be authorized. This request must be made to the Information Technology (IT) department one day prior to the scheduled visitation. Unescorted physical access to areas containing cardholder data is prohibited.

At the end of the visit, the receptionist will recover the temporary ID badge.

As part of the new employee orientation, Human Resources will distribute an Authorization Request Form and notify the Information Security department. The new employee's direct supervisor should sign the form and return it to the Information Security department. Once received, the Information Security department will either approve or deny the request for a new ID badge. If approved, the Information Security department will create and distribute the ID badge to the new employee. Whenever an employee is terminated, the

Information Security department must immediately disable badge access for said employee. Human Resources will be responsible for recovering the ID badge from the terminated employee.

12.2. Store, Inventory & Secure Media Containing Sensitive Data

All electronic media storage devices or hard copy materials containing sensitive or confidential information must be sufficiently protected by adequate physical access controls. Facility controls, such as locks and key passes, must be used to limit ease of access to systems storing sensitive or confidential information. As part of an annual risk assessment, the Information Security department will review the security of all storage locations to ensure sensitive data is adequately protected.

12.2.1. Hard Copy Media

Examples of hard copy materials include paper reports, fax transmissions, receipts etc. Storage of these materials is subject to the following guidelines:

- Removal of hard copy materials from Edgio offices is prohibited.
- Removal of hard copy materials from Edgio data centers or computer rooms is prohibited without prior approval from the Information Security department.
- Any hardcopy material containing consumer data (confidential or sensitive) must be stored only at approved Edgio facilities/offices, and only for the minimum time necessary.
- Any hardcopy material containing confidential or sensitive material must be clearly labeled.
- All hardcopy media containing confidential or sensitive information must be securely stored in a locked container. Lockers, cabinets, storage bins and locked desks are acceptable, but must first be approved by the Information Security department. These materials are never to be stored in an unlocked or insecure container.

12.2.2. Electronic Media

Examples of electronic media includes CDs, DVDs, floppy disks, hard disks, USB thumb drives, backup tapes, etc. Any electronic media devices that store confidential or sensitive information must follow these guidelines:

- Confidential or sensitive information must not be copied to removable storage devices without prior consent from the Information Security department.
- Except for computer system backups, no electronic media is to be removed from Edgio facilities without prior consent from the Information Security department.
- Any electronic media containing consumer data (confidential or sensitive) must be stored only at approved Edgio facilities/offices, and only for the minimum time necessary.
- Any electronic media containing confidential or sensitive material must be clearly labeled and stored in a secure fashion.
- Incoming or outgoing media devices are to be delivered only via secured courier or other method approved by the Information Security department.

12.2.3. Media Inventory

Any storage devices utilized for archival or backup purposes must be retained in a secure environment. Only Edgio personnel and the contracted storage facility personnel should have access to the storage devices.

A Media Inventory Log must be kept in the same storage location as all hardcopy and electronic media used for data backups. On an annual basis, an inventory of all stored media and devices will be performed. Utilizing the Media Inventory Log, the Information Security department will compare the list of in-use media with records kept at the approved storage facility.

A member of the Information Security department must perform an annual inspection of this backup storage facility to ensure that the backups are secured and stored in a fireproof manner. This check will ensure that all security controls are in place and operational.

A unique tracking code must be applied to any storage vessel or shipping container used for transporting backup media with sensitive or confidential information. These devices must be registered with the Information Security department prior to the transfer.

Any storage device containing sensitive or confidential data must be identified as such prior to the transfer. The Information Security department must pre-approve potential media couriers and transport personnel.

During all media transfers, the personnel responsible will complete a Backup Media Transfer Log. The log must clearly indicate what media has been transferred, and by whom. The log must also include where the media is being transferred to, and a manager of the approved storage facility must sign the log upon receipt.

12.3. Data Disposal Policy

After sensitive or confidential data is no longer required for legal, regulatory or business needs it must be purged from Edgio systems using a method described within this policy. This policy pertains to all data either stored in Edgio systems, within temporary files or stored on external devices/drives.

All marked shred bins (for hard copy materials) must be locked prior to shredding. Edgio employees should cross-cut shred any hardcopy material containing confidential or sensitive information as soon as possible.

The Information Security department must establish an automatic deletion process to be executed on cardholder information systems. This automatic process will occur on a nightly basis and will remove any sensitive or confidential data that is no longer required or has exceeded its usefulness.

Data stored in files or directories containing reusable information must be removed using a wiping program approved by the Information Security department.

External media storage devices containing confidential or sensitive data must be disposed of in a secure manner. This includes:

- Hard Disks: Perform a 7-pass binary wipe, degauss, or shred platter.
- Floppy Disks: Incinerate, shred, or melt.
- Tape Storage: Degauss, incinerate, shred, or melt.
- USB Drives (or "Thumb Drives"), Smart Cards and Digital Media: Incinerate, or melt.
- CDs and DVDs: Destroy surface, incinerate, shred, or melt.

All confidential or sensitive data must be deleted or otherwise destroyed prior to any Edgio computer equipment being shipped to a repair facility or other vendor for sale or trade-in.

Floppy drives, optical disks or other removable computer storage devices may not be donated to charity or recycled.

If Edgio outsources the disposal of media or computer equipment, only a bonded Disposal Vendor may be used. The vendor must provide a Certificate of Destruction to Edgio.

13. Secure Data Transmission

13.1. Transmission Over Untrusted Networks

To avoid interception or misuse of data, any confidential or sensitive information that is to be transmitted over public networks must be secured using strong encryption tactics, such as:

- TLS v1.2 with at minimum 2048-bit encryption
- Internet Protocol Security (IPSec) protocol
- Trusted keys/certificate authorities

Edgio wireless networks must be protected through the WPA2-Enterprise secure data encryption methods. Wireless systems shall not be used in the CDE or any customer-facing systems.

Credit card data will not be transmitted over chat (IRC, Slack, etc.), email, social networks or any other insecure transmission mechanism.

13.2. End User Messaging Technologies

Employees may never email unencrypted confidential or sensitive information such as credit card PANs. If a valid business justification exists, the Information Security department will supply encrypted email software to said employee. In addition, employees shall never send unprotected PANs via other messaging technologies such as instant messaging, chat or text.

14. Special Tech Use Policy

This policy must be followed by all users of special Edgio technologies, whether employees, contractors or third parties. Exemptions may only be authorized with written approval from the Chief Security Officer.

"Special technologies" refers to wireless networks, modem use and access, and any other employee-facing technologies used within the Edgio computing environment. This policy will be updated in the future to reflect new special technologies and their intended uses.

14.1. Approval





Integration or use of special technologies must be authorized by the Information Security department, based on job function. In regard to the general user, this applies to dial-in modem access, personal modem deployment, and wireless network access. Approvals must be documented using the Authorization Request Form.

14.2. Authentication

Wherever possible, user authentication mechanisms must be incorporated into Edgio authentication systems. User authentication requirements must adhere to the strict policies and procedures as currently defined for passwords (complex passwords, password change process, etc.). A strong two-factor authentication scheme (approved by the Information Security department) must be used if a user is remotely accessing the Edgio network using special technologies.

14.3. Device Inventory

The Information Security department must pre-approve personal modems and wireless network interfaces and log these devices using the Special Technologies Device Inventory. Users of these technologies must also be approved by the Information Security department and noted on the Special Technologies User List. The following users must be documented:

-  Vendors with dial-in modem access
-  Employees with dial-in modem access
-  Personal modem users
-  Wireless network users

14.3.1. Device Identification

Each of these approved devices, including personal modems and wireless access points, must be labeled with the device owner, contact information and the device's purpose/business function.

14.3.2. Acceptable Use

The guidelines and restrictions listed in the Acceptable Use Policy also apply to the acceptable use of Edgio special technologies.

14.3.3. Permitted Locations

The placement/installation of wireless access points and dial-in modems must be authorized by the Information Security department. Dial-in modems should be maintained in a location where they are free from tampering. Wireless access devices should be installed in the ceiling plenum. The use of these devices must be logged in the Special Technologies Device Inventory and the Special Technologies User List.

14.3.4. Approved Products

The Information Security department must approve devices before they are installed onto the Edgio network. The use of approved devices must be logged in the Special Technologies Device Inventory and the Special Technologies User List.

14.3.5. Session Disconnect

Modems (dial-in or modem banks) must be configured to automatically disconnect a user after 30 minutes of inactivity.

14.3.6. Vendor Connections

Any modem used solely by a third-party vendor for maintenance or support must remain disconnected until required. The Information Security department must approve the activation of these modems or create a management procedure to handle the task. The modem must be disabled immediately upon completion of the task.

14.3.7. Credit Card Data Access

It is forbidden to store cardholder data on local hard drives, floppy disks or other external storage media. All access to systems that are PCI in-scope must go through the Edgio VPN.

15. System Configuration Policy

This policy applies to all Edgio-operated servers and network devices, whether supervised by employees or third parties. All devices must have vendor-supplied defaults changed prior to deployment. Exemptions may only be authorized with written approval from the Information Security department.

15.1. Wi-Fi Access Point Vendor Defaults

Edgio wireless networks must have default configurations changed at installation. Examples of vendor defaults that need to be changed at installation are:

- wireless encryption keys
- passwords
- SNMP community strings

Edgio wireless networks must be protected through secure data encryption methods, such as WPA or WPA2 (if supported). Default settings using WEP as a key exchange protocol should never be used, as WEP is considered an insecure protocol. The minimum encryption strength for wireless networks is 128 bits.

Wireless encryption keys and shared secrets are to be changed at least once every 90 days, or whenever an employee with knowledge of the keys is terminated or leaves the organization.

15.2. System Configuration Standards and Deployment

Edgio configuration standards for all system components must be maintained in accordance with industry-accepted system hardening standards.

15.2.1. Applicability

Edgio production systems run on a custom Amazon Linux 2 AMI which has been hardened against CIS Amazon Linux 2 Benchmark version 1.0.0. The build scripts for this AMI are kept in a Github repository, are updated regularly, and are tested for compliance by the AWS Inspector CIS rules package on a weekly cadence.

All production instances must adhere to these requirements.

15.3. System Purpose

Edgio computing systems should adhere to a 'one primary function per resource' rule. For example: web servers, database servers and DNS should be operated from distinct and separate servers. Unless otherwise required by vendor documentation, no multi-purpose system may store, transmit, or process sensitive or confidential information. If Edgio implements virtualization technology, for example, multiple virtualized server instances on the same physical host; the virtual servers must be treated as individual server boundaries and thus secure configurations must be implemented to restrict communication between each other.

15.3.1. Remove Unnecessary Services/Systems

Only secure services, protocols and daemons that are necessary for a system to function are permitted. Functionality of system components should at all times match an up-to-date 'System Configuration Record' form that Edgio maintains for all system component types. If any systems are configured to use insecure services, protocols or daemons, there must be a business justification to do so, and additional security features must be documented and implemented in accordance with vendor-supplied documentation.

15.4. System Security Configuration Process

The following are process guidelines to be followed during new system deployments:

1. Provision new instance using latest image.
2. Update operating system software. This is automatically done whenever a new AMI is built. Production instances should be rotated regularly to use the latest stable AMI.
3. Configure OS parameters to properly secure the system. As stated in the System Configuration Standards and Deployment section above, our AMIs are hardened according to CIS benchmarks.
4. Install software and applications.
5. Configure application parameters according to build documentation.
6. Enable logging as per the Logging & Auditing Policy. Further, Amazon Inspector and CloudWatch should both check to ensure logging is configured properly on each running instance, and that logs are being sent.
7. FIM (File Integrity Monitoring) software should be installed for systems containing sensitive or confidential information.
 - Configure the FIM software to perform critical file comparisons on a weekly basis. This will alert the Information Security department in the event of unauthorized modification of any critical system files.

15.4.1. Required Software

All Edgio systems must install the following list of standard software. Any deviation or exemption from these configuration standards must include a reasonable business justification and an Edgio risk assessment. The deviation must then be approved by the Information Security department and logged in the System Configuration Record for the specific system.

15.5. Physical Servers/Windows Systems





Anti-virus software

15.6. "Critical Path" Systems

File integrity monitoring software

15.7. Edgio/Personal Computers

All Edgio-issued computers, as well as personal computers containing Edgio data or information, must have Hardware Management installed and always enabled, which manages the following:

-  Personal firewall
-  VPN client/configuration
-  Anti-virus software
-  Full-disk encryption

16. System & Apps Security Policy

16.1. Security Patches

When a vendor releases security patches, hot fixes and/or service packs, it is the Information Security department's responsibility to apply the changes as needed.

Third-party system components used in the production environment should be protected from known vulnerabilities by having the latest vendor-supplied security patches installed.

Critical security patches must be installed within 30 days of their initial release. Edgio has planned maintenance windows on the first week of each month to apply all pending security updates. Critical patches will be evaluated and deployed as soon as possible.

16.2. Vulnerability Identification & Risk Assessment

Any issues or vulnerabilities related to Edgio systems must be reported to the Information Security department. Once identified, the Information Security department is responsible for alerting system administrators and all relevant personnel.

AWS Inspector runs weekly in each region, checking each Edgio production system against a list of known CVEs. If an unpatched instance is found, the Information Security department is informed.

All Information Security personnel are required to review the following for new or updated vulnerabilities:

- AWS Security Bulletins
- Snyk Vulnerability DB
- RubyGems
- npm

Once a vulnerability is identified, the risk that vulnerability poses must be evaluated and ranked. This will allow the Edgio Information Security department to address high priority risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. Edgio uses the Common Vulnerability Scoring System (CVSS) v2.0 calculator to determine the risk ranking for those vulnerabilities that are lacking a vendor-supplied patch classification.

Any vulnerability identified as high risk is immediately scheduled to be patched within 30 days, and earlier if possible.

Edgio System Configuration Standards must be updated to reflect all new vulnerabilities and the measures required to remediate them.

16.2.1. PCI-impacting Network and System Changes

Upon completion of any significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.

16.2.2. Secure Software Development Best Practices

It is important to consider the control measures and security checks that will be used throughout the software development life cycle. Proprietary software developed by Edgio, whether internally or by a third party, must utilize industry best practices for software development.

16.2.3. Develop & Test Web Apps Based on Secure Coding Guidelines

We use the OWASP Secure Coding Practices Quick Reference Guide to train developers in secure coding techniques. All developers attend annual training sessions where we discuss security issues. The Platform team developers are aware of common coding vulnerabilities and the training guide on <http://www.owasp.org>.

Vulnerability	Mitigation
Injection flaws, particularly SQL injection	Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.
Buffer overflow	Validate buffer boundaries and truncate input strings.
Insecure cryptographic storage	Prevent cryptographic flaws.
Insecure communications	Properly encrypt all authenticated and sensitive communications.
Improper error handling	Do not leak information via error messages.
All "high-risk" vulnerabilities (as identified in PCI DSS Req. 6.2)	Mitigate as cases arise.
Cross-site scripting (XSS)	Validate all parameters before inclusion, utilize context-sensitive escaping, etc.
Improper Access Control	Properly authenticate users and sanitize input. Do not expose internal object references to users.

Cross-site request forgery (CSRF)	Do not reply on authorization credentials and tokens automatically submitted by browsers.
Broken authentication and session management	N/A

16.2.4. Software Firewall System

Edgio's software is split into 2 distinct sections: the Edgio Platform, and compiled transformation scripts (or "slugs"). The Platform refers to the core proxy code that runs in production (as well as some modules). Compiled transformation scripts are used to configure the Platform. The proxy itself acts a software firewall and transformations cannot impact security. Please note that secure parameters (such as logging, secure authentication, etc.) are handled by only the Platform code.

Only Platform engineers can commit to the proxy code that runs in production. Almost all development cycles will be completed entirely without any effect on system architecture, and therefore without any effect on security.

In addition, we have strict privilege separation on all production instances. The Platform is run as a unprivileged user, and that user cannot write to directories ensuring that code that runs cannot modify itself.

16.2.5. Bug Fixes

Platform engineers and Security Administrators are present at scrum meetings. Any features that might be a detriment to security are redesigned. All changes to architecture must be approved by the Head of Information Security, who is intimately familiar with all PCI requirements.

16.2.6. Testing

Any software changes must be tested to meet PCI-DSS requirements prior to deployment. Requirements to test against include:

- proper error handling
- secure cryptographic storage
- secure communications
- proper use of Role-Based Access Control (RBAC)

16.2.7. Release Process

The Platform has regularly scheduled releases. Issues are filed and tracked in ClickUp, managed each team lead, and fixed as soon as possible. The team lead waits for confirmation from the engineers stating that they have reviewed all code and a release is ready for release; code reviews must ensure code is developed according to secure coding standards.

The following is a high-level overview of the various security measures to be utilized during each phase of Edgio's software development:

- Requirements Analysis: The developer is responsible for determining whether application requirements are sufficiently secure.
- Design: All application components must be developed in accordance with the latest data and network security trends.
- Development: The developer is responsible for considering vulnerabilities that might affect the application, such as privilege/access bypass and memory bound issues.
- Code Review: To better identify security issues, a second developer is responsible for conducting code reviews of all new or updated software.
- QA Implementation: It is important that the QA process does not hamper security controls or introduce new issues or vulnerabilities.
- QA Testing: The application's security features must be thoroughly tested, along with functional and efficiency testing.
- Documentation: Directions for correct security configurations must be included with all software feature guides and implementation/installation documentation.
- Production Implementation: It is important that the implementation process does not hamper security controls or introduce new issues or vulnerabilities.
- Production Testing: The application's security features must be thoroughly tested, along with functional and efficiency testing.

- Maintenance: New code must undergo the same reviewing/testing process as outlined above. Any future application maintenance must not hamper security controls or introduce new issues or vulnerabilities.

16.2.8. Address New Threats/Vulnerabilities for Public-facing Apps

Our public-facing web site is in scope in our annual penetration test and goes through application vulnerability security assessment. Refer to the latest penetration test in our security documentation.

16.2.9. Ensure Security Policies & Procedures Documented/In Use

Personnel need to be aware of and following security policies and operational procedures to ensure systems and applications are securely developed and protected from vulnerabilities on a continuous basis.

Any Edgio applications that are considered web-based must be given special consideration. While these web-based applications must adhere to the same security measures outlined in the Development Life Cycle section, additional vulnerabilities must also be reviewed and tested.

Secure coding training is mandatory for all Edgio developers, and their development process must consider the OWASP guidelines. These guidelines are available at the following website: <http://www.owasp.org>

During the Code Review and Testing phases, the following vulnerabilities must be checked:

1. Insecure Configuration Management
2. Unvalidated Input
3. Denial of Service
4. Malicious Use of User IDs
5. Insecure Storage
6. Malicious Use of Account Credentials and Session Cookies
7. Error Handling Flaws
8. Cross-site Scripting
9. SQL Injection and other Command Injection Flaws
10. Buffer Overflows
11. Cached routes with potentially sensitive data, and their TTL's

The Edgio Platform is a stateless system that does not store any data and not currently susceptible to items 2, 5, 6, or 9 in the list above. For all other items, unit tests should be in place.

As part of the Code Review for Insecure Configuration Management, reviewers must ensure that all secrets and sensitive information are not in code nor committed to SCM.

On an annual basis, or whenever modifications have occurred, the web-based applications must undergo penetration testing performed by a third-party vendor. All custom code must be reviewed by an application security firm or have established an application layer firewall in front of web-facing applications.

Code running on the Edgio Platform is owned by the respective Edgio customer, and they are responsible for the security and testing of their code, as all the business logic resides on the original web site and not in the transformation logic.

16.2.10. Change Management/Control

Separate development/test and production environments

Development and test environments are distinct from production environments. The production environment is in a separate AWS account, with no access allowed between the production and the development accounts.

Separation of duties

The Platform team handles production. Non-platform team members do not have access to production, only to dev boxes.

Live PANs not used for testing

We do not have live PANs. Never used for testing.

Remove test accounts from production

Production never has test accounts at all. It is created fresh, with no data in it.

Remove custom accounts before release

We don't create custom accounts in production at all. Production is totally distinct from development environments, and is created from scratch.

Documentation of impact

Before pushing a release, the Engineering team confirms that all code has been reviewed.

Documented change approval by authorized parties

Once a version of the Platform code has been marked as "release ready" on our internal console, the Platform and Security Team ensures that all security criteria have been met. That version can then be pushed to production.

Functionality testing to verify that the change does not adversely impact the security of the system

After platform code passes all tests, we start the deployment process.

Back-out procedures

Releases are accomplished by deploying an approved build number. Back-out procedures are generally simple: switch back to previous version. Our internal tools log which version have been deployed. The previous build number can be found in the deployment logs and is used in case there is a need to roll back.

17. Top 10 Vulnerabilities

Edgio engineers are trained in secure coding techniques using the OWASP Secure Coding Practices Quick Reference Guide and the 2017 OWASP Top 10 Application Security Risks.

1. Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization. Our platform performs no business logic; not susceptible to injection flaws.

Edgio Risk: N/A; our platform performs no business logic; not susceptible to injection flaws.

2. Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

3. Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

4. XML External Entities (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

5. Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

6. Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

7. Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

8. Insecure Deserialization




Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

9. Using Known Vulnerable Components

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or

Data and information are among Edgio's most valuable assets. Edgio's Data Classification and Use Policy addresses the need to properly classify, control, and handle data and sensitive information to prevent its unauthorized use, disclosure, and modification.

The policy is designed to:

-  Protect the privacy of customers and employees
-  Protect the confidentiality of business information and intellectual property
-  Ensure compliance with application statutory, regulatory, and contractual obligations regarding the management and security of information

18. Document Information

Effective Date	Distribution	Classification	Owner
25 May 2023	Edgio Internal	Confidential	Edgio InfoSec

Version History

Version	Contributor(s)	Date	Activity
1.0	Julie Villarreal, Tech Writer	12 May 2023	Draft original document
	Darrin Reynolds, CISO	25 May 2023	Review/Approve document