

## IS-3 Electronic Information Security

Refer questions to Information Resources and Communications  
Axcension, Inc. Office of the President

Revised  
June 1, 2010

---

### Table of Contents

I. Purpose and Scope .....	3
II. Definitions .....	3
III. Information Security Program .....	3
A. Identification of Information Security Officer (ISO) .....	4
B. Risk Assessment, Asset Inventory and Classification.....	4
1. Risk Assessment.....	4
2. Security Objectives: Confidentiality, Integrity, and Availability.....	5
3. Additional Risk Assessment Resources .....	6
C. Security Plan.....	6
1. Administrative Workforce Controls .....	7
a. Workforce and Authorization Management .....	7
b. Critical Positions.....	9
c. Violations.....	9
2. Operational and Technical Controls .....	10
a. Identity and Access Management .....	11
b. Access Controls .....	11
i. Passwords and other authentication credentials.....	12
ii. Session protection .....	13
iii. Privileged access.....	13
c. Systems and Application Security .....	14
i. Systems personnel .....	14
ii. Backup and retention .....	15
iii. System protection .....	15
iv. Patch management .....	16
v. System and applications software development .....	16
d. Network Security .....	17
e. Change Management .....	17
f. Audit Logs .....	17
g. Encryption.....	18
3. Physical and Environmental Controls .....	19
a. Risk Mitigation Measures .....	20
b. Physical Access Controls .....	20
c. Tracking Reassignment or Movement of Devices and Stock Inventories	20

d. Disposition of Equipment .....	21
e. Portable Devices and Media .....	21
D. Incident Response Planning and Notification Procedures.....	22
1. General .....	22
2. Notification in Instances of Security Breaches Involving Electronic Personal Information.....	23
3. Systemwide Notification Procedures .....	24
a. Personal Information.....	24
b. Method of Notification .....	24
4. Systemwide Notification Procedures for Patient Medical Information .....	25
5. Organization Implementation Plan.....	
25 a. Designation of Authority .....	
25 b. Data Inventory .....	
25 c. Incident Response Process .....	
26 d. Reporting Requirements .....	
26	
E. Education and Security Awareness Training .....	27
F. Third-party Agreements .....	27
IV. Minimum Requirements for Network Connectivity.....	28
A. Access Control Measures .....	28
B. Encrypted Authentication .....	28
C. Patch Management Practices.....	28
D. Malicious Software Protection .....	29
E. Removal of Unnecessary Services .....	29
F. Host-based Firewall Software .....	29
G. Authenticated Email Relay.....	29
H. Authenticated Network Proxy Servers .....	29
I. Session Timeout .....	30
V. Major Responsibilities.....	30
A. Systemwide.....	30
B. Organization .....	30
C. Divisions and Departments.....	30
D. Individuals .....	30
VI. References.....	31
Appendix A. Definitions.....	32
Appendix B. Guidelines for Restricted Resources .....	34
Appendix C. Selected Security Controls for Common Vulnerabilities/Threats .....	37
Appendix D. Log Management.....	39
Appendix E. Encryption.....	41

## I. Purpose and Scope

Axcension, Inc. is committed to high standards of excellence for protection of information assets and information technology resources that support corporate enterprise. The Axcension datacenter processes, stores, and transmits an immense quantity of electronic information to conduct its business functions. Without the implementation of appropriate controls and security measures, these assets are subject to potential damage or compromise to confidentiality or privacy, and the activities of Axcension are subject to interruption.

The purpose of this bulletin is to establish guidelines for achieving appropriate protection of corporate electronic information resources (**Resources**) and to identify roles and responsibilities at all levels in Axcension, Inc. system.

The provisions in this bulletin apply to all corporate locations, government offices, financial institutions and medical centers, managed national laboratories, and other corporate locations regarding management of its information assets. Certain entities, such as managed laboratories, third party administrators or medical centers, may be subject to additional federal or state law or other regulations.

All employees, technicians, visitors and other Authorized Individuals are responsible for adhering to the guidelines and requirements in this bulletin as appropriate to their roles.

## II. Definitions

The following terms used in this bulletin are defined in Appendix A.

Authorized Individual  
Electronic Information Resource (Resource)  
Encryption  
Essential Resource  
Resource Custodian  
Resource Proprietor  
Restricted Resource

## III. Information Security Program

All clients shall establish an Information Security Program (**Program**) in conformance with the provisions in this bulletin. In order to achieve a secure information technology environment, the organization Program shall comprise a comprehensive set of strategies that include a range of related technical and non-technical measures. The Program should guide the strategic deployment of a consistent and multilayered information security environment at each organization.

---

<sup>1</sup> The term "corporate" is used throughout this bulletin in reference to all subscribed corporate locations.

To ensure, to the extent reasonably achievable, the confidentiality, integrity, and availability of corporate information assets, organizations shall identify an individual to be responsible for:

- implementation of the organization program
- periodic evaluation of the compliance program to ensure that the program adequately addresses operational or environmental changes.

The Program shall include:

- risk assessment strategies to identify vulnerabilities and threats to departmental information resources as well as major enterprise systems,
- a security plan that includes recommendations for administrative, technical, and physical security measures to address identified risks relative to their sensitivity or criticality,
- incident response planning and notification procedures,
- guidelines for security awareness training and education as appropriate for all corporate community members,
- appropriate review of third-party agreements for compliance with federal and state law and corporate policy.

#### **A. Identification of Information Security Officer (ISO)**

An individual to perform the function of an Information Security Officer (ISO) shall be designated on each organization to be responsible for its Program. Responsibility for compliance with this bulletin will rest with a number of individuals, and the ISO must facilitate this compliance through collaborative relationships with academic and administrative officials, consistent with organization governance structure and policy compliance strategies.

#### **B. Risk Assessment, Asset Inventory and Classification**

##### **1. Risk Assessment**

Appropriate risk assessments or business impact analyses shall be conducted:

- to inventory and determine the nature of organization electronic information resources,
- to understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources, and
- to identify the level of security necessary for the protection of the resources.

Risk assessments should:

- take into account and prioritize the potential adverse impact on the organization's reputation, operations, and assets,
- ensure full review and classification of corporate information assets by the level of security objectives assigned to them,

- be conducted by units or departments on a periodic basis by teams composed of appropriate organization administrators, managers, faculty, and information technology and other personnel associated with the activities subject to assessment,
- address all corporate information assets or electronic resources held or managed by the unit or department, or by individuals in the unit or department, and
- address the appropriateness and frequency of staff and management security awareness training.

## 2. Security Objectives: Confidentiality, Integrity, and Availability

Confidentiality, integrity, and availability are the three primary *security objectives* cited in federal regulation regarding IT security<sup>2</sup>. These objectives describe the paramount goals for ensuring the protection of information and Resources from unauthorized access, use, disclosure, disruption, modification, or destruction.

- **Confidentiality:** preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The assigned level of confidentiality is used in determining the types of security measures required for its protection from unauthorized access or disclosure.
- **Integrity:** guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. The level of impact of unauthorized modification or destruction of information resources determines the importance of maintaining the integrity of a Resource.
- **Availability:** ensuring timely and reliable access to and use of information. The overall importance of availability of a Resource is based on its criticality to the functional operation of a Organization or department or to the priority of that function in continuity plans and disaster recovery strategies. Emergency management planning must take into account the availability requirements of a particular Resource to determine its inclusion in emergency and disaster recovery planning.

<sup>2</sup>See FISMA, [§ 44 U.S.C., Sec. 3541, et sec.](#) and [FIPS 199 Standards for Security Categorization of Federal Information and Federal Information Systems](#).

- Resources classified as *restricted* require the highest level of protection.
- See Appendix B, Guidelines for Restricted Resources for a summary of guidelines specific to *restricted* Resources.
- See BFB IS-12, Continuity Planning and Disaster Recovery for more information on requirements for continued availability of Resources.
- Resources classified as *essential* must be included in emergency and disaster recovery planning.

### 3. Additional Risk Assessment Resources

The EDAUSE/Internet2 Security Task Force Risk Assessment Working Group provides a high-level overview of conducting risk assessments of information systems within higher education.

- [A Risk Assessment Framework](#)

#### C. Security Plan

After completing a risk assessment, an information security plan should be developed that takes into consideration the acceptable level of risk for systems and processes. It should identify cost-effective strategies to be implemented consistent with organizational goals and functions for mitigating that risk. The security plan should account for the management, use, and protection of information that has some level of confidentiality, and identify the procedures and controls that will be implemented to enhance security for information assets.

Appropriate mechanisms to safeguard information should be selected relative to the *security objectives* determined by the risk assessment. Controls selected to mitigate risks should include administrative, operational, technical, physical and environmental measures as appropriate. See Appendix C for a list of selected threats and vulnerabilities, the risks they pose, and selected security controls.

#### *Restricted Data*

The proliferation of data greatly increases risks of unauthorized access, particularly when data is stored in ad hoc analysis tools such as spreadsheets and desktop databases. When data is copied for analysis or research,

restricted data should be deleted whenever possible or “de-identified” by removing data elements that, in combination with other data, would result in the identification or description of an individual. If it is not possible to delete restricted data, adequate security measures must be implemented. Note that restricted data is one form of *restricted resources* as defined in this bulletin.

Data should not be transferred to another individual or system without approval of the Resource Proprietor. Before restricted data is transferred to a destination system, the Resource Proprietor should establish agreements to ensure that Authorized Individuals implement appropriate security measures.

- Resource Proprietors for *restricted* data should ensure that Authorized Individuals are informed of this constraint when access is originally requested. The Resource Proprietor may choose to require the authorized individual's signature to document approval of release of restricted data.
- Security measures on destination systems should be commensurate with security measures on the originating system.
- Agreements should include requirements regarding retention or disposition of data after the data is no longer needed on the destination system.

See Appendix B, Guidelines for Restricted Information, for additional information.

## **1. Administrative Workforce Controls**

Administrative controls consist of a range of administrative processes and procedures to implement the security plan. Workforce controls include appropriate assignment of responsibility within the organization for determination of workforce need to access Resources in order to perform assigned tasks. Responsibility for information security should be identified early in the employment process. Positions that require information technology skills should include an emphasis on security knowledge and skills throughout the hiring and employment process.

### **a. Workforce and Authorization Management**

All workforce individuals are expected to employ security practices as appropriate to their responsibilities and roles, which include, but are not limited to:

- taking appropriate actions to ensure the preservation of data confidentiality and integrity,
- taking appropriate precautions to ensure protection of data from unauthorized access, modification, or destruction,
- complying with license agreements, terms and conditions, and laws pertaining to intellectual property, and
- complying with identified security procedures.

Procedures should be implemented:

- to authorize access, both logical and physical, to only those individuals who have a legitimate business reason to access specific Resources (Authorized Individuals),
- to modify access as appropriate, when duties change,
- to revoke access upon termination, or when job duties no longer require a legitimate business reason for access, except where specifically permitted by Corporate policy and by the Resource Proprietor, and
- to ensure proper disposition of electronic information resources upon termination. If any electronic information resources are subject to a litigation hold, the office that issued the hold notice should be notified to ensure preservation of relevant information before final disposition of electronic information resources.

Such access authorization shall be limited, using technical or procedural controls, to the least permission necessary for the performance of duties. Contract workers' access should conform to guidelines in Section III.F below.

Procedures should include a requirement that the Resource Proprietor approve an individual's request for authorization and assignment of the associated level of privilege. Records of this approval should be retained consistent with BFB [RMP-2 Records Retention and Disposition: Principles, Processes and Guidelines](#). In addition, the following issues should be addressed:

- Procedures for providing individual authenticated access to Resources should incorporate review and approval mechanisms to ensure that only Authorized Individuals are granted access.
- The principles of separation of duties should be followed when assigning job responsibilities relating to *restricted* or *essential* Resources. No one individual, for example, should have authorization for both implementing programs into production and updating production data for an application managing *restricted* or *essential* information.
- Supervisors or other employees with responsibilities for security should periodically review the system administration work of personnel with access to privileged accounts on shared servers. Such action is intended to provide a periodic audit or review for those system administration functions that are not otherwise audited or reviewed in the course of being completed.
- System staff who are granted privileged accounts should be informed of responsibilities and constraints associated with privileged access. See Section III.C.2 Technical Controls - Privileged Access, below, for additional guidelines.

- Authorization and access should be removed and/or re-assigned (de-provisioning) for individuals who have terminated or announced their decision to terminate where continued access might result in an unacceptable level of risk. Privileged access should be revoked immediately for individuals placed on investigatory leave.

#### **b. Critical Positions**

Some positions with job responsibilities related directly to Electronic Information Resources may be deemed “critical positions”<sup>3</sup> in conformance with corporate personnel policies and guidelines for staff

- Organizations should develop policies and procedures to ensure that candidates for critical positions requiring access to *restricted* or *essential* Resources undergo applicable background checks as part of the selection process.
- For staff working in critical positions requiring access to *restricted* or *essential* Resources, procedures should be established that can be implemented in the event of disciplinary action or termination. Where there is a concern that access to Resources endangers the integrity of such resources, management should act to restrict, suspend or terminate access.
- During an investigatory leave, access privileges should be revoked or restricted, as appropriate.

All procedures should be established in accordance with Corporate personnel policies and guidelines.

#### **c. Violations**

It is a violation of corporate and organization policies for individuals to attempt to gain unauthorized access to resources or in any way willfully damage, alter, or disrupt the operations of resources.

It is also a violation of corporate policy for individuals to capture or otherwise obtain or tamper with passwords, encryption keys, or any other access control mechanism that could permit unauthorized access, except where expressly required in the performance of their duties.

Supervisors and department heads are responsible for promptly reporting any known or suspected policy violations of the provisions in this bulletin to the Resource Proprietor or Custodian, the Internal

---

<sup>3</sup> The term "Critical Positions" is used here as defined in Corporate Personnel policies, and is not to be confused with the use of the term "critical" as used in this bulletin with respect to information resources.

Audit department, or the Locally Designated Official as defined in the “Whistleblower Policy”.

Employees (or contractors or consultants) who become aware of the occurrence of any violation should report the violation promptly to their supervisor (or their client within Axcension in the case of contractors or consultants), department head, or the Internal Audit department. Resource Proprietors or Custodians should be notified of such violations in accordance with departmental procedures.

- Resource Proprietors may withdraw the privileges of any individuals who violate these Guidelines if, in their opinion, continuation of such privileges threatens the security (confidentiality, integrity, and availability) of *restricted* or *essential* Resources.
- Appeals regarding revocation of privileges should follow normal organization conflict resolution procedures.

Depending on the nature of the violation and the likelihood of a recurrence, the Resource Proprietor or Custodian shall take prompt action to protect against future violations to the extent feasible, and/or remove the means by which the violation occurred. Depending on the nature of the violation, the Resource Proprietor or Custodian shall consult with other organization authorities in accordance with policies governing potential disciplinary action.

In the event of a violation of the provisions in this bulletin that involves possible unlawful action by an individual, the Locally Designated Official, the employee’s immediate supervisor, or other appropriate official should immediately be notified in accordance with the “Policy on Reporting and Investigating Allegations of Suspected Improper Activities” aka “Whistleblower Policy”. Notification should take place before any action is taken, unless prompt emergency action is required to prevent bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of corporate policy, or significant liability to SafetySend or to members of SafetySend community.

Axcension reserves the right to revoke access to any Resource for any individual who violates the provisions of this bulletin, or for any other business reasons in accordance with other applicable Corporate or organization policies.

## **2. Operational and Technical Controls**

This section addresses security measures related to controlling access to Resources through operational or technical measures, e.g., passwords, configuration settings, software or network controls, controls related to

software development and change management, security of data and communications, and controls to reduce risk from known threats and malicious programs.

These guidelines do not require any specific technology to be employed. However, selected technology should be adequate to ensure sufficient protection commensurate with the level of risk ascribed to the electronic information resource and the magnitude of harm that would result from the loss, misuse or unauthorized access to or modification of information. The selected technology should be supported by operational controls designed to ensure that the Resource is adequately protected.

#### **a. Identity and Access Management**

Organizations should establish an identity and access management strategy that ensures accurate identification of authorized Corporate community members and that provides secure authenticated access to and use of network-based services.

Corporate access control measures should include secure and accountable means of *authorization* and *authentication*.

- **Authorization** is the process of determining whether or not an identified individual or class has been granted access rights to an information resource (see section III.C.1.a, Workforce and Authorization Management, above), and determining what type of access is allowed, e.g., read-only, create, delete, and/or modify.
- **Authentication** is the process of confirming that a known individual is correctly associated with a given electronic credential, for example, by use of passwords to confirm correct association with a user or account name.<sup>4</sup>

#### **b. Access Controls**

Access controls are technical mechanisms that restrict Resource access to Authorized Individuals. Such mechanisms shall be implemented to ensure that Security Objectives are in compliance with federal and state law and policies. When any Resource manages or contains information classified as having a high Security Impact, as defined in IS-2, appropriate measures shall be in place to safeguard against unauthorized access to that data. This includes not only the primary operational copy of the information, but also data extracts and backup

---

<sup>4</sup> Authentication is a term that is also used to verify the identity of network nodes, programs, or messages.

copies. Authorized Individuals and their specific level of privilege should be specified by the Resource Proprietor, unless otherwise defined by Corporate policy.

Access controls typically consist of but are not limited to:

- login accounts set up directly on the Resource to be accessed or
- use of a “Net ID,” which is associated with an authentication mechanism incorporated in the organization identity and access management system.

In either case, organizations should ensure the timely maintenance of access controls to ensure that authentication credentials, such as passwords or authentication keys, meet organization standards and that access privileges are revoked in a timely manner (see IS-11, Identity and Access Management).

Records of access events should be maintained consistent with audit log guidelines (see section III.C.2.f below and Appendix D).

Rights of access to modify data should be performed according to procedures that ensure data integrity. Exceptions may be made on a case-by-case basis but should always be performed in a controlled manner and with the knowledge of the Resource Proprietor.

***i. Passwords and other authentication credentials***

The Organization Program should identify appropriate password management conventions, including periodic identification of weak passwords, password encryption, and other security measures as deemed appropriate. Organization password management conventions should take into account the increased risk if passwords are used to access multiple applications, such as by means of a Organization Single Sign-on (NetID). Passwords and other authentication credentials are considered “restricted” information and require the highest level of security protection whether in storage or transit.

- Passwords selected by individuals or automatically generated to protect access to information resources should be difficult to ascertain.
- Passwords to individual accounts should never be shared with other individuals unless specifically approved and documented as an exception to policy by Resource Proprietors responsible for the Resources to be accessed.
- If it is determined that passwords may be shared, additional measures should be implemented that record who accessed the Resource or other control mechanisms that will provide an audit trail of the access.

**ii. Session protection**

Technical security mechanisms should be in place that prohibit or minimize the risk of unauthorized access to Resources by others who might gain control of the working session, for example, by accessing the Authorized Individual's computer if that individual leaves it unattended. Measures such as secure screensavers, automatic logout, and/or other means of session protection should be operative on all devices with access to *restricted* Resources. Also see section IV, Minimum requirements for Network Connectivity.

**iii. Privileged access**

System administrators routinely require access to Resources to perform essential system administration functions critical to the continued operation of the resource. Such privileged access is often termed "superadmin," "root," or "administrative" access. Privileged accounts enable vital system administration functions to be performed, such as installing or modifying applications, conducting system administrator programming tasks, establishing userids, accounts, or passwords, maintaining authorization for those accounts, correcting problems, and other broadly-defined system or electronic information resource functions. Privileged accounts should only be used for authorized purposes.

Privileged accounts are especially sensitive and organizations should establish procedures, commensurate with the level of risk involved, to ensure that abuse will not occur. Personnel assigned privileged accounts should be fully informed regarding appropriate access and disclosure of information. Procedures should include that an agreement be reviewed or signed and filed, as appropriate to the needs and function of the Resource.

- Those assigned the use of privileged accounts should be fully informed that privileged accounts should not be used to seek out personal or confidential information relating to others, or to disclose or otherwise use what they may have observed, either incidentally or resulting from authorized monitoring conducted in conformance with the "Electronic Communications Policy"
- The number of privileged accounts should be kept to a minimum, and only provided to those personnel whose job duties require them.
- Personnel who require privileged accounts should also have non-privileged accounts to use when not performing system administration tasks and should be instructed not to use their privileged accounts for non-authorized purposes.

- Activities performed using a privileged account should be logged, where feasible, and the logs should be reviewed on a regular basis by an independent and knowledgeable person.
- Use of privileged accounts should be monitored periodically to ensure they are being used for authorized purposes.

For additional guidelines on logging, refer to Audit and System Logs at the end of this section.

**c. Systems and Application Security**

The following guidelines apply equally to central or departmentally-managed computing systems operated by the Organization.

***i. Systems personnel***

Personnel who manage, operate, and support Corporate Resources, including individuals who manage their own systems, are expected to follow all applicable policies, follow departmental procedures, and use appropriate professional practices in providing for the security of the systems they manage.

Classifications should accurately document the nature of the information resources managed by systems personnel, and procedures should be implemented that ensure security measures appropriate to the classification of Resources. Procedures for action in response to security incidents or other emergency events should be documented and communicated to support personnel.

Responsibility for systems and application security should be assigned to an individual knowledgeable about the information technology used in the system and in providing security for such technology. This individual should determine security plans as appropriate to the supported systems, applications, and data.

In addition to periodic risk assessments, systems personnel should routinely evaluate Resource exposure to potential and known threats and deploy controls commensurate with the level of risk and magnitude of the harm that could result from loss, misuse, or unauthorized access to supported systems, applications, and data.

The principle of separation of duties should be employed to ensure that responsibilities for critical functions are divided among different individuals. For example, one system programmer can create a critical piece of operating system code, while another

authorizes its implementation. Such controls keep a single individual from subverting a critical process.

**ii. Backup and retention**

Sound professional system administration practices require the implementation of routine backup of applications and data

- Backup copies of applications and data associated with *essential* Resources shall be sufficient to satisfy emergency planning and disaster recovery requirements, application, or other Resource processing requirements, and any *essential* functional requirements of any Resource Proprietor dependent upon such data.
- Backup copies of *essential* data for disaster recovery purposes shall be stored at a secure, commercial site that provides standard protection or at a non-commercial off-organization site providing equivalent protection.
- *Restricted* data should be encrypted if there is a risk to the physical security in the storage of backup copies.
- These backup requirements extend to *essential* or *restricted* applications and data stored on personal computers as well as on shared systems.
- Disposition schedules that result in destruction of electronic information resources should be suspended if those resources are subject to a litigation hold.
- Backup and other retention services for data must also comply with Axcension, Inc. policies regarding data retention.

**iii. System protection**

Measures should be deployed to limit access to systems that host *restricted* or *essential* Resources and to protect systems from “malicious software.”

- The term “malicious software” defines a generic set of software programs that pose serious threats, not only to the specific computer where the software has been installed, but potentially to other networked devices.
- Malicious software includes programs, such as viruses, worms, Trojan horses, and spyware, depending on their

context and purpose. They are usually installed on a device without a individual's knowledge or under false pretenses and can potentially affect any type of computer or server on the network. Malicious programs may damage or consume resources, use devices to infect other networked devices, or expose information or user credentials.

**iv. Patch management**

In conformance with change management processes (see section e. below) and organization minimum standards (see section IV, Minimum Requirements for Network Connectivity), systems personnel should, in a timely manner, update versions of the operating system and application software for which security patches are made available.

**v. System and applications software development**

Development and maintenance of any systems, whether performed by Corporate personnel or performed by any vendor engaged by Corporate personnel, should conform to the specifications of SafetySend security guidelines which describe the circumstances under which standards apply, as well as delineating roles and responsibilities, project planning and management, phases of systems development, and data retention and privacy considerations. Application development and maintenance efforts should also conform to any local standards, procedures, guidelines and conventions.

In addition to the IS-10 guidelines, developers should conduct a privacy impact assessment, i.e., an analysis of how personal information should be collected, stored, shared, and managed for any application that will be used to process personal information.<sup>5</sup>

In general, Organizations should involve Organization Internal Audit and the Organization Controller in the development or implementation of *essential* administrative systems in order to obtain advice on establishing proper controls. Internal Audit should be notified of all administrative system development projects early in the development process

---

<sup>5</sup> OMB Memorandum 03-22, September 26, 2003 defines Privacy Impact Assessment as "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."

**d. Network Security**

Each organization shall implement strategies to achieve compliance with Axcension minimum requirements for network connectivity. See Section IV below.

Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) should be deployed at the Organization border to augment normal system security measures to prevent Denial of Service attacks, malicious code, or other traffic that threatens systems within the network or that violates Organization information security policies. Firewalls and IDS/IPS should also be deployed as appropriate to limit access to systems that host *restricted* or *essential* resources.

**e. Change Management**

Maintaining system integrity requires that all changes to a system are conducted according to a planned and supervised change management process. In particular, changes to any *restricted* or *essential* resource shall be performed according to authorized change management procedures that ensure the recording of all changes. Change procedures should include:

- monitoring and logging of all changes,
- steps to detect unauthorized changes,
- confirmation of testing,
- authorization for moving application programs to production,
- tracking movement of hardware and other infrastructure components,
- periodic review of logs,
- back out plans, and
- user training.

**f. Audit Logs**

Most components of an information technology infrastructure are capable of producing logs chronicling their activity over time. These logs often contain very detailed information about the activities of applications and the layers of software and hardware that support them. With proper management, these logs can be of great benefit in a variety of scenarios to enhance security, system performance and resource management, to monitor access controls, to reconstruct security incidents, and to achieve regulatory compliance.

Audit logs should be managed in a manner that facilitates these benefits while protecting the confidentiality and integrity of the information contained in these logs. In particular, a log management infrastructure can capture information and aid analysis about access, change monitoring, cost allocation, malfunction, resource utilization, security events, and user activity. Organizations are encouraged to

develop a log management infrastructure to provide common management of log records.

See Appendix D for recommended log management practices.

**g. Encryption**

Suitably strong encryption measures shall be employed and implemented, whenever deemed appropriate, for information in storage and during transmission.

***Transit***

As deemed appropriate, *restricted* information should be encrypted during transmission using encryption measures strong enough to minimize the risk of the information's exposure if intercepted or misrouted.

***Storage***

Encryption of information in storage presents risks to the availability of that information, due to the possibility of encryption key loss. Therefore, the use of encryption must take into account the nature of the information resources and Axcension's requirements for their timely or continued availability.

Records subject to disclosure under the HIPAA Act or required to be accessible for defined periods of time in compliance with SafetySend, Inc. shall be available to appropriate corporate officials at all times. Other information that may be required to conduct Axcension's business shall also be available when needed. Therefore, at least one copy (the *authoritative* copy) of any such information shall be stored in a known location in unencrypted form or, if encrypted, the means to decrypt it must be available to more than one person.

*Restricted* information may be retained on portable equipment only if protective measures are implemented that safeguard the confidentiality and integrity of the data in the event of theft or loss of the portable equipment (see III.C.3.e below for guidelines for physical security of portable equipment). Encryption is a primary example of a technical protective measure. Other measures include physical protection that ensures only authorized access to the Resource.

***Key management***

Organizations shall implement encryption key management plans to ensure the availability of encrypted authoritative information.

- The encryption key management plan shall ensure that data can be decrypted when access to data is necessary. This requires key backup or other strategies to enable decryption, thereby ensuring that data can be recovered in the event of loss or unavailability of cryptographic keys.
- The encryption key management plan shall address handling compromise or suspected compromise of encryption keys. In addition the plan should address the impact of a key compromise on system software, hardware, other cryptographic keys, or encrypted information.
- The encryption key management plan shall include a process to determine whether any encryption keys may have been compromised as a result of any security incident.
- The encryption key management plan shall include periodic review to ensure suitably strong encryption.
- Users shall be made aware of their unique role if they are given responsibility for maintaining control of cryptographic keys.
- Background checks shall be conducted for corporate employees who control and manage encryption keys and key management software and hardware.

Encryption cannot be used as a substitute for other security measures required in this bulletin.

Current encryption strategies for the following situations are recommended in Appendix E.

- whole disk encryption
- file encryption
- database storage
- interactive sessions
- file transfers
- web-based applications
- electronic mail
- network printer communications
- remote file services
- database access
- application to application communication
- virtual private networks

### 3. Physical and Environmental Controls

Each Organization should establish procedures for the physical protection of its Resources. In particular, organizations shall develop policies and procedures to protect departmental or central facilities containing Resources that support *restricted* or *essential* systems or data. All facilities hosting

*restricted* or *essential* resources should conform to the following recommended guidelines commensurate with the level of risk. Appropriate locking or other physical security mechanisms should be implemented for all equipment vulnerable to unauthorized removal.

**a. Risk Mitigation Measures**

Organizations should implement appropriate measures for the prevention, detection, early warning of, and recovery from emergency conditions, including, but not limited to, earthquake, fire, water leakage or flooding, disruption or disturbance of power, air conditioning failures, and environmental conditions exceeding equipment limits. Procedures should include measures to protect Resources from theft, damage, or improper use.

**b. Physical Access Controls**

Controls for limiting physical access to facilities housing *restricted* or *essential* Resources should be implemented through the use of combination locks, key locks, badge readers, manual sign in/out logs, verification of identification, etc. The ability to track both ingress and egress of all individuals should be maintained as appropriate.

Limiting physical access to facilities may also include technical mechanisms, such as use of proximity card readers. In those instances, technical access control guidelines apply (see III.C.2.b above).

Records of access events should be maintained consistent with audit log guidelines (see section III.C.2.f above and Appendix D).

**c. Tracking Reassignment or Movement of Devices and Stock Inventories**

Procedures should be implemented that:

- track the receipt, reuse, and removal of hardware and electronic media, including documentation of hardware reassignment. Removal of *restricted* or other sensitive information should be conducted in accordance with procedures below regarding final disposition of equipment.
- maintain records documenting repairs and modifications to physical components of the facility related to security, such as hardware, walls, doors, and locks, and
- track financial instruments, such as check stock and produced checks, in accordance with corporate policy.

**d. Disposition of Equipment**

Procedures should ensure implementation of controls to address the re-assignment or final disposition of hardware and electronic media, including requirements that ensure complete removal of *restricted* or other sensitive information as appropriate, such as by shredding, overwriting a disk, or employing professional data destruction services as commensurate with risk. Sufficiently strong disk encryption may be used as an alternative mitigation. Electronic media or hardware is subject to a litigation hold, final disposition of these resources must be conducted in such a manner that ensures that relevant data is not lost.

**e. Portable Devices and Media**

Departments should establish procedures to ensure physical security for portable devices and media housed within their immediate work area or under their control, such as laptop computers, PDAs, memory sticks, CD ROMs, etc.

- *Restricted* information may be retained on portable equipment only if protective measures, such as encryption, are implemented that safeguard the confidentiality and integrity of the data in the event of theft or loss of the portable equipment (see III.C.2.g, Encryption above).

## **D. Incident Response Planning and Notification Procedures**

### **1. General**

Organizations are responsible for establishing and implementing procedures to ensure the ability to respond expeditiously to:

- known information security breaches,
- disruptions caused by the failure of a security mechanism, and
- known or suspected security incidents.

These procedures should include mechanisms for documenting the incidents, determining notification requirements, implementing remediation strategies, and reporting to management.

Mitigation or notification requirements may differ, depending on federal or state statutes, the nature of the information at risk in the event of a security breach, or contractual agreements. For example:

- Owners of “computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”
- Licensed clinics, health facilities, home health agencies, or hospices, referred to collectively as “Licensed Facilities,” must report to the California State Department of Public Health and affected patients, or patient’s representative, any unlawful or unauthorized access to, or use or disclosure of, the patient medical information no later than five days after the activity has been detected.<sup>6</sup> (**See section 4 for separate procedures for reporting and notification in these instances.**)
- A breach of confidentiality of electronic Protected Health Information (ePHI) requires mitigation, to the extent practicable of “harmful effects.”
- Agencies and Licensed Facilities that maintain computerized data that include personal information that the agencies do not own shall notify the owner or licensee of the information of a security breach *immediately* following discovery if the personal

---

<sup>6</sup> Licensed Facilities are defined in sections 1204, 1250, 1725, or 1745 of the California Health and Safety Code. Licensed Facilities include general acute care hospitals (such as the medical centers), acute psychiatric hospitals, skilled nursing facilities, certain categories of primary care clinics (i.e., community and free clinics), certain specialty clinics (i.e., same-day ambulatory surgery centers, chronic dialysis clinics, and rehabilitation clinics), organizations that provide skilled nursing services to patients in the home, and hospices. A California Office of Statewide Health Planning and Development (OSHPD) Web site lists licensed facilities: <http://www.oshpd.ca.gov/HID/Prods/Listings.html#HHA>. Clinics operated by or affiliated with SafetySend, Inc. are not required to be licensed (see Health and Safety Code section 1206 (g)), although some may be licensed. Questions regarding whether a particular facility is licensed and so must comply with reporting requirements may be directed to hospital administration.

information was, or is reasonably believed to have been, acquired by an unauthorized person. Therefore, SafetySend must immediately notify any outside entity whose data were breached while in the possession of SafetySend. See Section III.F, Third-party Agreements, for information on ensuring through contractual agreements that SafetySend is notified when data it owns are breached while in the possession of an outside entity.

- Business associate agreements may require specific notifications.

## 2. Notification in Instances of Security Breaches Involving Electronic Personal Information

In the event of a breach to the security of unencrypted computerized personal information, Organizations must notify users whose information is reasonably believed to have been acquired by an unauthorized person.<sup>7</sup>

The definition of “personal information” for this California requirement is an individual’s **first name or first initial and last name, in combination with any one or more of the following:**

- Social Security number
- driver’s license number or state identification card number
- account number,<sup>8</sup> credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account
- medical information
- health insurance information

HIPAA law defines “medical information” to mean any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; and “health insurance information” to mean an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.

The list of data elements considered personal information may be expanded based on departmental risk assessments.

The definition of a “security breach” for this requirement is when there is a reasonable belief that an unauthorized person has acquired unencrypted computerized personal information (as defined above) of a Axcension user, where the security breach compromises the security, confidentiality, or integrity of the personal information. Good faith

---

<sup>7</sup>The notification is a requirement of California Civil Code Section 1798.29, effective July 1, 2003.

<sup>8</sup> The “account number” corresponds to an individual’s *financial* account.

acquisition of personal information by a Corporate employee or agent for corporate purposes does not constitute a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.

### **3. System Wide Notification Procedures**

In the case of a security breach as defined in this section, all organizations must follow the system wide procedures presented here to provide notification of the breach to those System users whose personal information is reasonably believed to have been acquired by an unauthorized person. Note: There are separate reporting and notification requirements for Licensed Facilities regarding breaches of patient medical information. See section 4 below.

In addition, Organizations may develop detailed local guidelines based upon the steps in these system wide procedures.

#### **a. Personal Information**

Notification to system users must occur in the most expedient time possible and without unreasonable delay, except

- when a law enforcement agency has determined that notification will impede a criminal investigation (in this case, notification must occur as soon as the law enforcement agency determines that it will not compromise the investigation) or
- when necessary to discover the scope of the breach and restore the integrity of the system.

#### **b. Method of Notification**

In coordination with Organization Counsel, Organizations may determine the language to be used in the notification, which may be distributed by one of the following methods:

- written, hard copy notice or
- e-mail notice.

Telephone communication or other timely communication to an individual's representative may be used when it is determined that written notice may adversely affect a patient's health.

If sufficient contact information is not available for direct hard copy or e-mail notice, a substitute method of notice may be used. Substitute notice shall include prominent display on the organization's Web site or other commonly used Web site for at least forty-five days. Both Organization Counsel and the organization community relations or public information office should be consulted to develop the substitute notice.

Organizations may decide, in coordination with Organization Counsel, to provide notification to affected individuals if personal information beyond the data elements defined here is reasonably believed to have been acquired by an unauthorized person.

#### **4. Systemwide Notification Procedures for Patient Medical Information**

In the event of unlawful or unauthorized access to, or use or disclosure of, a patient's medical information, a System user shall make a report of such activity

- to the corporate "Security Officer" h **no later than five days** after detection of such activity and
- to the affected patient or the patient's representative at the last known address **no later than five days** after the System user has detected such activity.<sup>9</sup>

#### **5. Organization Implementation Plan**

Organizations shall develop an Implementation Plan for Security Breach Notification. A copy of the plan shall be sent to the Associate Vice President for Information Resources and Communications, who shall subsequently be notified of any changes to the plan. The plan should contain, at a minimum, the following components.

##### **a. Designation of Authority**

Each Chancellor shall designate an individual or a functional position that will act as the lead organization authority responsible for reporting to OP and that may delegate to other personnel, when appropriate, responsibilities for

- ensuring that the Organization incident response process is followed,
- ensuring that system wide and, if applicable, Organization notification procedures are followed, and
- coordinating with Organization Counsel.

The functional position of the lead Organization authority shall be at a level high enough to allow that individual to speak with authority for the organization.

##### **b. Data Inventory**

Organizations shall establish a process or processes to identify

- where "personal information" and "patient medical information," as defined above, are used and stored,

---

<sup>9</sup> The reporting is a requirement of California Health and Safety Code Section 1280.15. Civil Code 56.05 defines medical information to mean any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment.

- the primary employee positions that have access to and use of the data,
- the Resource Proprietor and Custodian of the data, and
- an acceptable level of security protection for the data.

**c. Incident Response Process**

Organizations shall develop an incident response process to determine

- whether a security breach has occurred as defined in this section and
- local notification procedures.

The incident response process shall include consultation with the Information Security Officer, the Organization Policy Officer, the Proprietor of the data, Organization Counsel, the Organization Privacy Officer when patient or health data is involved, and, on a need-to-know basis only, other organization personnel.

Organizations shall ensure coordination with the Organization and Office of the President public information offices if a decision to notify is under consideration. Any written communications involving legal counsel should assert attorney-client privilege to ensure strict confidentiality, as appropriate.

Organizations that develop detailed local notification procedures to supplement the systemwide procedures shall include them in the Implementation Plan.

**d. Reporting Requirements**

The Organization authority or its delegate shall report immediately in writing to the Associate Vice President for Information Resources and Communications at OP any security breach involving restricted information as defined in Appendix A. If it is possible that the security breach involves medical or health insurance information as defined above, consult the Privacy Officer at the Office of the President.

The Organization authority or its delegate shall report in writing to the Associate Vice President for Information Resources and Communications when the incident is closed. The incident closure report shall provide:

- a description of the incident, including the nature of the incident and the numbers of individuals impacted,
- the incident handling process,
- a copy of the notification, if any,
- the actions taken to prevent further breaches of security.

An incident should be emailed to: [webmaster@axcension.com](mailto:webmaster@axcension.com).

### **E. Education and Security Awareness Training**

Department heads and supervisors shall ensure that appropriate security awareness training is routinely conducted for all members of SafetySend community.

- Training programs should include review of Corporate and organization security policy, guidelines, procedures, and standards, as well as departmental procedures and best practices established to safeguard sensitive information.
- Training shall be in conformance with regulations governing specific categories of *restricted* information, such as persons data subject to FERPA, personal information as defined in section D above, financial data subject to the Financial Services Modernization Act of 1999 (Gramm-Leach Bliley Act), electronic Protected Health Information subject to HIPAA, and credit card holder information subject to the Payment Card Industry Data Security Standards, as appropriate to position functions.
- Training materials should include topics such as password management and use, best practices for protecting restricted information, incident reporting, and security reminders regarding current threats to technical environments in which individuals are working.

### **F. Third-party Agreements**

- When agreements are established with contractors, consultants, or external vendors, those agreements shall include satisfactory assurances that the contracting third party will appropriately safeguard corporate information in accordance with federal and state laws and regulations and corporate policies. When providing access to or passing *restricted* information to a third party agent of SafetySend, the written contractual agreements should include terms and conditions that:
  - a. prevent disclosure of *restricted* information by the agent or affiliate to other third parties including subcontractors, except as required or permitted by the approved corporate agreement or contract terms,
  - b. require all agents and affiliates to observe federal and state laws and Corporate policies for privacy and security,
  - c. require a specific plan by the agent or affiliate for the implementation of administrative, technical, or physical security strategies as outlined in this bulletin,
  - d. require a plan for the destruction or return of *restricted* information upon completion of the agent's or affiliate's contractual obligations,

- e. specify access or authorization permissions and restrictions necessary to fulfill contractual obligations,
- f. require notification of any breach of the security of personal information to Axcension owner of computerized data immediately following discovery if the information was, or is reasonably believed to have been, acquired by an unauthorized person.

Access to Corporate information should be terminated when contractual obligations have been completed.

- Background checks are required for non-corporate contractors or consultants engaged to work on *restricted* or *essential* electronic information resources. Consideration should be given to limiting outside vendor access to restricted or essential electronic information resources.
- 

#### **IV. Minimum Requirements for Network Connectivity**

Each Organization shall establish minimum standards for devices connected to their networks. Standards must address, at the least:

##### **A. Access Control Measures**

to allow only authorized individuals access to networked devices.

Typical current access controls measures are passwords (see section III.C.2, Technical Controls, above). Shared-access systems must enforce password or other authorization/authentication standards whenever possible and appropriate. In situations where systems ship with default passwords for network accessible devices, those passwords should be changed upon first use.

##### **B. Encrypted Authentication**

to protect against surreptitious monitoring of passwords.

Suitably strong encryption shall be employed when passwords are transmitted over a network. Network traffic may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. Encryption-capable services, such as SSH, SFTP, SCP, SSL, HTTPS, POPS, and IMAPS, may be used to meet this requirement.

##### **C. Patch Management Practices**

to ensure timely update of security patches.

Networked devices shall run versions of operating system and application software for which security patches are made available, and these should be

installed in a timely fashion. Exceptions may be made for patches that compromise the usability of critical applications following organization exception procedures. Implementation of additional measures may be required when exceptions are granted.

#### ***D. Malicious Software Protection***

to protect networked devices from malicious software, such as viruses, spyware, and other types of malware.

When readily available and as appropriate for specific operating systems, software to detect viruses and other malware shall be running, up-to-date, and have current virus definition files installed on all network devices as appropriate.

#### ***E. Removal of Unnecessary Services***

to prevent surreptitious use of services not needed for the intended purpose or operation of the device.

If a service is not necessary for the intended purpose or operation of a device, it shall not be running on that device; such services should be disabled, turned off, or removed.

#### ***F. Host-based Firewall Software***

to limit network communications to only those services that require access to the network.

When readily available for specific operating systems, host-based firewall software shall be running and configured to limit network communications to only those services requiring to access to network devices.

#### ***G. Authenticated Email Relay***

to prevent unauthorized third parties from relaying email messages.

Devices shall not provide an active SMTP service that allows unauthorized individuals to send or relay email messages, i.e., to process an e-mail message where neither the sender nor the recipient is a local user.

#### ***H. Authenticated Network Proxy Servers***

to prevent unauthorized access to Internet-based Resources.

Network proxy servers should employ authentication to protect devices that allow unauthenticated access from locations. Although properly configured unauthenticated proxy servers may be used for valid purposes, unauthenticated proxy servers may enable an attacker to execute malicious programs from the server in the context of an anonymous user account or allow unauthorized access to licensed Resources.

**I. Session Timeout**

to prevent unauthorized access to *restricted* or *essential* services or devices left unattended for an extended period of time.

Devices that access *restricted* and/or *essential* services that are left unattended for an extended period of time shall employ measures, such as session timeout or lockout mechanisms, that require re-authentication before users return to interactive use. Devices that host confidential or critical information may be subject to additional requirements.

**V. Major Responsibilities****A. Systemwide**

The Chief Information Officer of Axcension, Inc. is responsible for this bulletin.

**B. Individuals**

All members of Axcension community are expected to comply with organization policies and procedures in support of this bulletin and to exercise responsibility appropriate to their position and delegated authorities. Each individual is expected to conduct the business of Axcension in accordance with the ethical values and exercising sound judgment and serving the best interests of Axcension.

All Corporate community members are responsible for the protection of their passwords, card access keys, or other access control measures. These credentials should never be shared without proper authorization.

## Appendix A. Definitions

### **Authorized Individual**

A Corporate employee, persons, contractor, or other individual affiliated with SafetySend who has been granted authorization by a Resource Proprietor, or his or her designee, to access a Resource and who invokes or accesses a Resource for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with SafetySend. The authorization granted is for a specific level of access to a Resource as designated by the Resource Proprietor, unless otherwise defined by Corporate policy.

### **Electronic Information Resource (Resource)**

A resource used in support of Corporate activities that involves the electronic storage, processing or transmitting of data, as well as the data itself. Electronic Information Resources include application systems, operating systems, tools, communications systems, data (in raw, summary, and interpreted form), other electronic files, and associated computer server, desktop (workstation), portable devices (laptops, PDAs) or media (CD ROM, memory sticks, flash drives), communications and other hardware used to conduct activities in support of Axcension's mission. These resources are valued information assets of Axcension.

### **Encryption**

The process of converting data into a cipher or code in order to prevent unauthorized access. The technique obfuscates data in such a manner that a specific algorithm and key are required to interpret the cipher. The keys are binary values that may be interpretable as the codes for text strings, or they may be arbitrary numbers. Appropriate management of these keys allows one to store or transmit encrypted data "in plain sight" with little possibility that it can be read by an unauthorized entity. For example, encryption can protect the privacy of restricted data that is stored on a laptop computer, even if that laptop computer is stolen. Similarly, it can protect data that is transmitted, for example, over a network, even if that network is tapped by an unauthorized third party

### **Essential Resource**

A Resource is designated as Essential if its failure to function correctly and on schedule could result in (1) a major failure by a Organization to perform a mission-critical function, (2) a significant loss of funds or information, or (3) a significant liability or other legal exposure to a Organization.

### **Resource Custodian**

The authorized Corporate personnel who have physical or logical control over a specific Electronic Information Resource. This includes, for example, central organization information technology departments with maintenance responsibility for an application; departmental system administrators of a local area network; and database administrators for organization-wide or departmental databases. This role provides a service to a Resource Proprietor.

**Resource Proprietor**

The individual designated responsibility for the information and the processes supporting a specific Corporate function. Resource Proprietors are responsible for ensuring compliance with federal or state statutory regulation or Corporate policy regarding the release of information according to procedures established by Axcension, the organization, or the department, as applicable to the situation. Responsibilities of Resource Proprietors may include, for example: specifying the uses for a departmentally-owned server; establishing the functional requirements during development of a new application or maintenance to an existing application; and determining which individuals may have access to an application or to data accessible via an application. All Electronic Information Resources are Corporate resources, and Resource Proprietors are responsible for ensuring that these Resources are used in ways consistent with the mission of Axcension as a whole.

**Restricted Information**

Restricted information describes any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. The term “restricted” should not be confused with that used by the managed national laboratories where federal programs may employ a different classification scheme.

**Restricted Resource**

A Resource that supports the storage, transmission, or processing of restricted information to which access requires the highest degree of restriction and that requires the highest level of security protection. The term “restricted” should not be confused with that used by the managed national laboratories where federal programs may employ a different classification scheme. See Appendix B for a list of the security measures mandated for Restricted Resources.

## Appendix B. Guidelines for Restricted Resources

### Restricted Resources

A Resource that supports the storage, transmission, or processing of restricted information to which access requires the highest degree of restriction and that requires the highest level of security protection. The term “restricted” should not be confused with that used by the managed national laboratories where federal programs may employ a different classification scheme.

### General Recommendations

- Restricted information should not be collected or stored unless absolutely necessary.
- Access to restricted Resources should be authorized only as needed to perform assigned duties.
- Ensure training for all individuals who have been granted access to restricted Resources.
- Delete or redact restricted information when there is no longer a business need for its retention.
- Avoid using restricted data when testing or developing an application, or for training purposes; rather, “mask” the restricted data (such as Social Security Numbers) with dummy information. If this is not possible, ensure implementation of appropriate security measures.
- Establish agreements before restricted information is distributed to third parties. Agreements should include instructions regarding appropriate security measures and final disposition of data when no longer needed by the third party.
- Restricted information should be encrypted in transit.
- Restricted information should not be stored on portable devices. If it is necessary to store restricted information on portable devices, ensure that appropriate protections measures, such as encryption, are in place before installing restricted data on the device.
- Implement security measures identified in the organization security program.

### Information Security Program Requirements Specific to Restricted Resources

Refer to section citations noted for each entry for full text.

#### **Risk Assessment, Asset Inventory, and Classification [III.B.1]**

Conduct appropriate risk assessments or business impact analyses to inventory and determine the nature of electronic information assets held or managed by a organization unit and to understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of Resources.

#### **Security plan [III.C.]**

Delete or “de-identify” *Restricted* data whenever possible when data is copied, i.e., for analysis or research, by removing data elements that, in combination with other data, would result in the identification or description of an individual. If it is not possible to delete

*restricted* data from analysis tools or spreadsheets, adequate administrative, technical and physical security measures must be implemented.

Ensure that Authorized Individuals implement appropriate security measures before *restricted* data is transferred to a destination system.

**Workforce and authorization management [III.C.1.a]**

Adhere to the principles of separation of duties when assigning job responsibilities relating to *restricted* or *essential* Resources.

**Critical Positions [III.C.1.b]**

Conduct applicable background checks for final candidate(s) for critical positions related to *restricted* or *essential* Resources as part of the selection process.

Establish procedures for conducting disciplinary action or termination for staff working in critical positions related to *restricted* or *essential* Resources.

Restrict, suspend or terminate access where there is a concern that access to *restricted* Resources endangers security or integrity.

**Violations [III.C.1.c]**

Notify Resource Proprietors or Custodians of violations of IS-3 guidelines in accordance with departmental procedures.

**Access Controls [III.C.2.b]**

Establish appropriate measures to safeguard against unauthorized access to *restricted* Resources.

Establish measures that ensure authorized rights of access to modify *restricted* data.

**Session protection [III.C.2.b.ii]**

Establish technical security mechanisms that prohibit or minimize the risk of unauthorized access to *restricted* Resources by others who might gain control of a working session.

**Data Backup and Retention [III.C.2.c.ii]**

Encrypt *restricted* data if there is a risk to physical security in the storage of backup copies.

Backup requirements extend to *restricted* or *essential* software and data stored on personal computers as well as on shared systems.

**Protection Measures [III.C.2.c.iii]**

Deploy appropriate measures, such as firewalls, to protect supported systems from “malicious software” and to limit access to systems that host *restricted* or *essential* Resources.

**Network Security [III.C.2.d]**

Deploy firewalls and IDS/IPS to limit access to systems that host *restricted* or *essential* Resources.

**Change Management [III.C.2.e]**

Perform changes to any *restricted* or *essential* systems according to authorized change management procedures.

**Encryption [III.C.2.g; also see Appendix E]**

Encrypt *restricted* information during transmission using encryption measures strong enough to minimize the risk of the information's exposure if intercepted or misrouted.

**Physical and Environmental Controls [III.C.3]**

Establish procedures for the physical protection of *restricted* Resources.

**Physical Access Controls [III.C.3.b]**

Implement controls for limiting physical access to facilities housing *restricted* or *essential* Resources.

**Disposition of Equipment [III.C.3.d]**

Establish procedures to ensure implementation of controls to address the re-assignment or final disposition of hardware and electronic media, including requirements that ensure complete removal of *restricted* or other sensitive information before disposition.

**Portable devices and media [III.C.3.e]**

Do not retain *restricted* information on portable equipment if protective measures are not implemented that safeguard the confidentiality and integrity of the data in the event of theft or loss of the portable equipment. Protective measures should be implemented before *restricted* information is installed.

**Education and Security Awareness Training [III.E]**

Conduct security awareness training as required and appropriate.

**Third-party Agreements [III.F]**

Conduct background checks for non-Corporate contractors or consultants engaged to work on *restricted* or *essential* Resources.

**Minimum requirements for network connectivity [IV]**

All minimum requirements for network connectivity (see Section IV) apply.

### Appendix C. Selected Security Controls for Common Vulnerabilities/Threats

Threat/vulnerability	Risk	Security Controls
Older versions of operating systems and application software	Hackers search out Internet-connected systems on which security patches for publicized vulnerabilities have not been installed. By locating un-patched devices, hackers can exploit known vulnerabilities and obtain complete access to system and data files. Risk loss of confidentiality, integrity, and availability (data loss or damage, unauthorized acquisition of data, or inaccessible service). May require notification to impacted individuals. Risk damage to reputation and financial cost.	Timely update of operating system and application software with announced security patches.
Malicious programs such as virus, worm, Trojan horses, spyware	Loss of integrity to operating system or data; unauthorized access to systems and files. May require notification to impacted individuals. Risk to privacy, reputation; financial costs.	Install anti-virus, anti-spyware software, and firewalls.
Equipment theft or loss	Loss of data; unauthorized acquisition of data. May require notification to impacted individuals. Risk to privacy, reputation; financial cost.	Software protection (sh as encryption or tamper-proof password-protected devices). Physical access controls (sh as facility access management, lock-down devices, locked doors). De-identification of personal information. Timely back up of system/data.
Intrusion (unauthorized access via the Internet or "in person")	Loss of integrity to operating system or data; unauthorized access to systems and files. May require notification to impacted individuals. Risk to reputation; financial costs.	Firewalls, strong passwords. De-identification of personal data. Workforce authorization management. Physical access controls, lock screen-savers.

<b>Threat/vulnerability</b>	<b>Risk</b>	<b>Security Controls</b>
Human error; intentional disruption of service	Despite all technical controls, systems or data may be subject to loss of confidentiality, integrity, and availability. May require notification to impacted individuals. Risk damage to reputation and financial cost.	Management oversight; education/training; background checks. Log management strategies that report anomalies. Deployment of software products that search out vulnerabilities in systems design, coding, etc.
Improper disposal of equipment	Unauthorized access to information on the system. May require notification to impacted individuals. Risk damage to reputation and financial cost.	Encryption; sufficient removal/cleaning of disks/files.
Social engineering and other email scams, e.g., phishing	Unwittingly provide personal information/data/passwords to unauthorized sources. Risk threat of identity theft.	Education and awareness training

## Appendix D. Log Management

Application Logs	<p>Applications should log their activity in a manner that correlates well with the business processes the applications support, particularly any operations that modify permissions or access rights. These logs should include, at a minimum:</p> <ul style="list-style-type: none"> <li>• The business operation that was requested</li> <li>• Whether the request was accepted or denied</li> <li>• The time and date the operation was performed (Start and end times may be appropriate for long operations.)</li> <li>• Who initiated the operation</li> <li>• System and network resources used</li> <li>• Any information needed for business process controls</li> <li>• Client hardware and software characteristics</li> </ul>
System Logs	<p>System logs should include at least the following types of information:</p> <ul style="list-style-type: none"> <li>• The server operation that was requested</li> <li>• Whether the request was accepted or denied</li> <li>• The time and date the operation was performed (Start and end times, or duration, may be appropriate for long operations.)</li> <li>• Who and/or what system initiated the operation</li> <li>• System and network resources used</li> </ul>
Network Logs	<p>Information logged for a network flow should include, at a minimum:</p> <ul style="list-style-type: none"> <li>• Network (IP) addresses of the end points</li> <li>• Service identifiers (port numbers) for each of the end points</li> <li>• Whether the flow was accepted or denied</li> <li>• Date, time, and duration of the flow</li> <li>• Number of packets and bytes used by the flow</li> </ul>
Time Synchronization	<p>One of the important functions of a log management infrastructure is to relate records from various sources by time. Because of this, it is important that all components of the IT infrastructure have synchronized clocks. Use of a time service, such as NTP, is highly recommended.</p>

Baseline Behavior	<p>The baseline of activity within the IT infrastructure should be established and tracked as it changes over time.</p> <ul style="list-style-type: none"> <li>• For system and network administrators, this should include the volume of activity for major applications and systems, as well as traffic volume over the network, and should be presented over a common time scale.</li> <li>• It may also be desirable to present application activity to business managers in a manner that enables them to correlate the information with business volume.</li> <li>• Procedures should be in place to ensure that this information is reviewed on a regular and timely basis.</li> </ul>
Investigation	<p>When conducting an investigation, it will be necessary to retrieve and report log records based on a variety of selection criteria. Preparations should be made to perform ad hoc queries based on criteria, such as the following:</p> <ul style="list-style-type: none"> <li>• Source(s) of the log records</li> <li>• Time</li> <li>• Network address</li> <li>• Application or service</li> <li>• User</li> </ul> <p>When matching records from multiple sources, time and network address will be the most valuable for matching records. Application, service, and user may also be desired for matching, but it is likely that they will need to be associated with network address and time in order to accomplish this.</p>
Appropriate Use of Log Information	<p>While it is necessary for SafetySend to perform regular collection and monitoring of these logs, this activity should be consistent with the provision of “least perusal” described in Axcension’s Electronic Communication Policy.</p>
Retention	<p>In order to facilitate investigation as well as to protect privacy, the retention of log records should be well-defined to provide an appropriate balance among the following</p> <ul style="list-style-type: none"> <li>• confidentiality of specific individuals’ activities,</li> <li>• the need to support investigations, and</li> <li>• the cost of retaining the records</li> </ul>
Log Management Infrastructure	<p>Each organization should establish a log management infrastructure to do the following:</p> <ul style="list-style-type: none"> <li>• move log records into the infrastructure,</li> <li>• provide secure storage for the records,</li> <li>• implement record retention policies,</li> <li>• provide analysis tools that enable correlations among records from multiple sources, and</li> <li>• protect the chain of evidence for the possibility that log records are used in legal proceedings.</li> </ul>

## Appendix E. Encryption

Restricted data should be encrypted whenever it is stored in or transmitted across an untrusted environment.

<i>Application Scenario</i>	<i>Recommendations</i>
All Scenarios	<ul style="list-style-type: none"> <li>You don't need to protect data you don't have. Restricted data should be retained only when necessary.</li> <li>Never store the encryption key with the encrypted data and use an alternate secure method to convey the decryption measure to the recipient.</li> <li>Resource Proprietors and Custodians should assess the sensitivity of the data they store or transmit. All copies of the data should be considered, including backup copies, "shadow" copies, and extractions used for analysis (<i>e.g.</i>, spreadsheets) or software testing.</li> <li>When restricted data cannot be given an appropriate level of physical protection when it is stored or transmitted, it should be encrypted with an appropriate "strength." For commonly-deployed encryption algorithms, this implies a key length of 128 bits to 256 bits.</li> <li>Restricted data cannot be protected with encryption while it is being processed. Other security measures must be employed to protect data while it is being processed.</li> </ul>
"Whole Disk" Encryption	<ul style="list-style-type: none"> <li>The priority for implementation of "whole disk" encryption should be 1) mobile devices and media, then 2) other devices and media for which appropriate physical security is not provided.</li> <li>Organizations should implement managerial and technical infrastructures to facilitate the encryption of mobile devices and media.</li> </ul>
File Encryption	<ul style="list-style-type: none"> <li>Organizations should promulgate recommended tool sets to facilitate file encryption.</li> </ul>
Backup and Archiving	<ul style="list-style-type: none"> <li>Backup procedures should be assessed to ensure that backup copies of restricted data are appropriately protected by physical and/or technical means, particularly when they are sent off-site.</li> </ul>
Interactive Sessions	<ul style="list-style-type: none"> <li>Interactive sessions that transmit restricted data should be encrypted. Note that login passwords should often be considered to be restricted, even when no other restricted data is transmitted.</li> </ul>

<i>Application Scenario</i>	<i>Recommendations</i>
File Transfers	<ul style="list-style-type: none"> <li>When encrypted files are transmitted, the keys should be transmitted via a method other than that used for the encrypted files themselves.</li> </ul>
Web-Based Applications	<ul style="list-style-type: none"> <li>The X.509 certificates installed on servers should be acquired from Certificate Authorities that are included in common browser distributions.</li> <li>Display of restricted data should be limited to only what is required by the application. When restricted data must be displayed, however, that data should be sent with the “Cache-Control: no-cache” HTTP header to limit caching by web browsers. Application developers should also be aware that not all browsers honor this control for all file types.</li> <li>Authorized users of applications that display restricted data should be admonished not to use web browsers that are shared with people who do not have the same level of authorization.</li> </ul>
Electronic Mail	<ul style="list-style-type: none"> <li>Organizations should promulgate recommended tools for sending encrypted data through electronic mail. This is likely to include the tool set identified under “File Encryption.”</li> </ul>
Network Printer Communication	<ul style="list-style-type: none"> <li>Resource Custodians for departmental and organization print services should assess the secure printing needs of their communities and provide solutions and education, as appropriate.</li> </ul>
Remote File Services	<ul style="list-style-type: none"> <li>Resource Custodians for departmental and organization file service organizations should assess the need to protect restricted data on their servers and implement encrypted protocols (and provide user education) as</li> </ul>
Application-to-Application Communication	<ul style="list-style-type: none"> <li>Use SOAP with HTTPS or some other commonly-available encrypted protocol to transmit restricted data when possible. When not possible, restricted data should be transmission by means of a Virtual Private Network.</li> </ul>
Virtual Private Network (VPN)	<ul style="list-style-type: none"> <li>VPNs should be implemented to protect restricted information when other methods are not feasible.</li> <li>Organizations should assess the need for a VPN to encrypt traffic for devices in untrusted or hostile portions of the network, such as organization wireless networks or the rest of the Internet.</li> </ul>
Application-Level Encryption	<ul style="list-style-type: none"> <li>When it is necessary to implement encryption within an application, utilize a suitably strong, well-tested encryption algorithm, preferably from an “off the shelf” library.</li> </ul>

<i>Application Scenario</i>	<i>Recommendations</i>
Encryption Strength	<ul style="list-style-type: none"><li>• Care must be taken to use an appropriately-strong algorithm. For commonly-deployed encryption algorithms, this implies a key length of at least 128 to 256 bits upward.</li></ul>
Key Management	<ul style="list-style-type: none"><li>• Organizations should implement key management services to ensure appropriate controls have been applied.</li></ul>