Legly
Information Security Program

V1.0

18/6 2021

Table of Contents

History

Version	Date	Author	Modifications
1.0	6/18/2021	SW	- First Version
			-
			-
			-

1.0 INFORMATION SECURITY MISSION STATEMENT

Legly and Legly employees have an inherent responsibility to protect the physical information assets of the company as well as confidential member data and intellectual capital owned by the company. These critical assets must be safeguarded to mitigate any potential impacts to the company or its customers. Information Security is, therefore, a critical business function that should be incorporated into all aspects of our business practices and operations.

To achieve this objective, policies, procedures, and standards, have been created to ensure secure business practices are in place at Legly. Information security is a foundational business practice that must be incorporated into planning, development, operations, administration, sales and marketing, as each of these business functions requires specific safeguards to be in place to mitigate the risk associated with normal business activities.

2.0 INFORMATION SECURITY POLICY OVERVIEW

Everyone at Legly is responsible for familiarizing themselves with and complying with all Legly's policies, procedures and standards dealing with information security.

Information security is: "The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats."

Information Security centers on the following three objectives for protecting information: Confidentiality, Integrity, and Availability. The policies in this document support these objectives.

2.1 Philosophy of Protection

Legly's philosophy of protection provides the intent and direction behind our protection policies, procedures, and control. Our protection philosophy is comprised of three tenets:

1. **Security is everyone's responsibility**. Maintaining an effective and efficient security posture requires a proactive stance on security issues from everyone. Security is not "somebody else's problem;" being part of Legly means you have the responsibility to adhere to the security policies and procedures of the company and to take issue with those who are not doing the same.

2. **Security permeates the Legly organization**. Security is not just focused on physical and technical "border control." Rather, we seek to ensure reasonable and appropriate levels of security awareness and protection throughout our organization and infrastructure. There is no place in our business where security is not a consideration and that is especially true for the development team.

3. **Security is a business enabler**. A strong security foundation, proactively enabled and maintained, becomes an effective market differentiator for our company. Security has a direct impact on our viability within the marketplace and must be treated as a valued commodity.

The tenets of our philosophy of protection are mutually supportive; ignoring any one tenet in favor of another undermines the overall security posture of our organization.

2.2 Critical Success Factors

The following factors are critical to the successful implementation of security within Legly:

- Comprehensive security policies, objectives and initiatives that clearly reflect our business objectives
- A security approach that is consistent with our culture
- Highly visible support from the executive management
- Solid understanding of security requirements and risk management practices, especially in regards to key customer data (e.g. contracts)
- Effective communication and guidance of security to all our managers, associates, partners, clients, vendors and developers
- Information security awareness and training
- Continual review and measurement of the effectiveness and efficiency of security controls and mechanisms
- Annual review of the information security policy to update policy as needed to reflect changes to business objectives or the risk environment.

2.3 Information Security Policy Structure

Legly's Information Security Policies are structured in such a way to give flexibility as required by the business objectives and needs, as well as making sure key customer data (e.g. contracts) is secure. Frequently, the weakest link is the link that breaks the security chain and causes a breach in security. Through consistent application of Information Security across the company and tech stack, any weak areas are compensated for and the organization is stronger overall.

Information Security Policy follows this tiered structure:

- Information Security Mission Statement
- Information Security Policy
- Information Security Standards and Processes
- Information Security Specific Configurations and Procedures

The hierarchy lends support as you progress up the tiers and becomes more detailed as you progress down the tiers. In this way, all actions taken have a basis in policy and directly support the policy or policies they are governed by. To illustrate this hierarchy, descriptions of the various levels are given below.

Information Security Mission Statement – This is the overall management direction in regards to Information Security at Legly. It is broad in scope and sets the expectations for protecting the company's information resources. It is contained in this document.

Information Security Policy – This is the collection of policies that implement the overall guidance of the Mission Statement. Policies are somewhat broad but topical in nature (centered on specific Information Security topics). The Information Security Policies are contained in this document.

Information Security Standards and Processes – These are collections of standards and processes that are to be used to implement the given policy they reference. Standards may dictate a type of technology to use but may stop before naming a particular product (depending on the policy and standard subject). Processes will detail the steps to take to fulfill the goals of a particular policy. Standards and Processes will be published under separate titles and may be regionalized to fit the conditions at different locations (i.e., there may be one set of standards for a particular policy in the United States, and a different set in Germany). Standards and Process will clearly delineate where they apply.

Information Security Specific Configurations and Procedures – These are very specific details that support the implementation of the standards and processes given above. These will include specific products and configuration details, or step-by-step procedures to implement processes. These are very highly localized and will apply to the environment for which they were written (i.e., there may be a specific configuration for Sun systems that is different from Windows configurations. These will be published under separate titles where directed.

3.0 SECURITY POLICY

Legly Executive Management will provide direction for, approve, publish and communicate the merits of an Information Security Policy document. This Information Security Policy Document shall outline managements' approach to Information Security as well as providing the organization with a strong indication of the management's commitment to Information Security within Legly.

The purpose of this policy is to communicate the direction of the organization's Information Security Program by providing relevant, accessible and understandable definitions, statements and explanations.

The Information Security Policy Document shall:

- Define information security as well as its scope and importance in the organization.
- Include a statement of management's intent for information security.
- Include a statement of management's goals and principles of information security.
- Explain the organization's security policies, standards and compliance requirements, including:
    - Compliance with legislative and contractual requirements,
    - Security education and awareness commitment,
    - Consequences for security violations.
    - Prevention and protection against viruses and other malicious software attacks,
    - Commitment to well thought-out and effective business continuity management.
        - Outline specific responsibilities for information security management.
        - Outline policies and procedures for reporting security incidents.

          The Information Security Policy Document shall serve as a reference document that will lead to additional more detailed information when necessary.

3.1 Review and Evaluation

Management shall be the owner of this Information Security Policy Document. The owner of the document shall be responsible for maintaining and reviewing the policy based upon a defined review process. The policy shall be reviewed at least annually and updated in response to any changes that would affect the assumptions from the baseline risk assessment, such as significant security incidents, new vulnerabilities, new regulations or changes to the organization's infrastructure.

The reviews shall include an assessment of the policy's effectiveness based upon:

- The nature and number and impact of recorded security incidents;
- Cost and impact of controls on business efficiency; and
- Effects of changes to technology.

4.0 SECURITY ORGANIZATION

4.1 Information Security Infrastructure

The purpose of this policy is to protect all the information assets within the organization by allocating specific responsibilities for all such assets.

Management is responsible for the overall application of the Information Security policies.

Each individual asset will be tracked and have its risk assessed so that the appropriate security levels can be applied.

Each asset will have an “owner”, who may delegate responsibilities, but remains ultimately responsible for the asset(s).

The asset owner will:

- Identify and define all security processes for their asset(s);
- Document all security processes on their assets; and
- Clearly define and document all authorization levels of their assets

4.2 Security of Third Party Access

The developers will control authorization for *types* of access to information processing facilities by third parties based upon the reasons for that access.

A risk assessment will be carried out before any third party access is granted and will consider the reasons for access as well as the necessary controls to be put in place.

Access of third parties to Information Processing facilities will be clearly spelled out in contracts; this access includes the scope of access to physical, logical and network assets.

5.0 ASSET & DATA CLASSIFICATION AND CONTROL

The purpose of this policy is to determine the protective controls associated with each Legly information asset and to provide a foundation for all employees (and contractors, third parties, etc. who deal with information assets) to understand the security and handling of such assets.

Legly's data and asset classification system has been designed to support access to information based on the need to know so that information will be protected from unauthorized disclosure, use, modification, and deletion. Consistent use of this data classification system will facilitate business activities and help keep the costs for information security to a minimum. Without the consistent use of this data classification system, Legly unduly risks loss of member relationships, loss of public confidence, internal operational disruption, excessive costs, and competitive disadvantage.

Consistent Protection: Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology was used to handle it, or what purpose(s) it serves. Although this policy provides overall guidance, to achieve consistent information protection, all employees are expected to apply and extend these concepts to fit the needs of day-to-day operations.

5.1 Accountability for Assets

The purpose of this policy is to outline the methodology for identifying, classifying, and documenting assets in order to provide protection that is commensurate with the value and importance of each asset. All employees are expected to be familiar with and comply with this policy.

To maintain accountability for assets, we will compile a list of all its information assets and establish the relative value and importance of each asset.

This policy requires that all information systems be identified and documented with a program in place to manage assets company-wide. All assets associated with each information system shall be identified and documented with their risk and data classification, and location.

5.2 Information Classification

Asset classification is the process of assigning value to data in order to organize it according to its sensitivity to loss or disclosure. All information assets shall be classified, using a company-wide asset classification system. All data, regardless of its classification, will be protected from unauthorized alteration; this policy provides guidance on the proper handling of data.

This policy requires that all information assets be classified and labeled in a manner that allows the asset to be readily identified to determine handling and protection level for that asset.

Information assets shall be assigned a sensitivity classification by the asset information owner or their nominees, in accordance with the following classification definitions:

- **Confidential**: Highly Sensitive information requiring the highest degree of protection. Access to this information shall be tightly restricted based on the concept of need-to-know. Disclosure requires management's approval and, in the case of third parties, possibly a signed confidentiality agreement. If this information were to be compromised, there could be serious negative financial, legal, or public image impacts to Legly. Examples include personal data or customer contracts, etc.
- **Medium-risk**: Information that is related to Legly business operations, but not available for public consumption. This information shall only be disclosed to third parties if a confidentiality agreement has been signed. Disclosure is not expected to cause serious harm to Legly, and access is provided freely to all employees. Examples include policies and standards, operational procedures, details about propriety service or AI strategies/designs etc.

- **Public**: Information that requires no special protection or rules of use. This information is suitable for public dissemination. Examples include press releases, marketing brochures, etc.

Management is responsible for maintaining the policy and ensuring the infrastructure exists to support this policy.

	Public data	**Medium-risk data**	**Confidential data**
Risk degree	Low	Medium	High
Description	Data that can be either freely disclosed to the public or has little negative impact on Legly.	Information of medium importance that is not meant for public disclosure. Such as details about various proprietary service or AI strategies/designs.	Highly sensitive data absolutely not meant for public disclosure. Such as personal data or customer contracts.
Access rights	Low or nonexistent limitations.	Moderate access, mostly available to people on a need-to-know basis (for those who need this data to do their job)	Access only to very few relevant staff. Access is approved and controlled by management.
Potential impact	The negative impact from this data being leaked or published is inconvenient at most.	The negative impact from this data being leaked or published is potentially damaging to the company, but in a limited way.	The negative impact from this data being leaked or published is highly destructive, capable of creating both financial and lawful problems to the company.

5.2.1 Handling and Protection Rules

Each asset classification shall have handling and protection rules. These rules must cover any media the assets may reside in at any time.

All computer-resident confidential information shall be protected via access controls to ensure that it is not improperly disclosed, modified, deleted or otherwise rendered unavailable.

Unless it has specifically been designated as “Public”, or “Medium-risk”, all Legly internal information shall be assumed to be confidential and shall be protected from disclosure to unauthorized third parties.

No confidential information of Legly or of any third party shall be disclosed to the public or any unauthorized third party without the prior approval of Legly’s Management.

Handling and protection rules must include all parts of an asset’s life-cycle, from creation/installation through use and finally to destruction/disposal. Sensitive information or systems must be appropriately disposed of when no longer needed.

6.0 PERSONNEL SECURITY

6.1 Employment Security

6.1.1 Personnel Screening Policy

Legly conducts background checks to ensure the safety of existing employees and to ensure that the employees we hire possess the highest possible level of integrity and business ethics.

The purpose of this policy is to assure that information assets are protected from personnel that may not be trustworthy of the responsibilities associated with security protection and handling.

All screening and supervision shall be in accordance with appropriate legislation in the relevant jurisdiction.

6.1.2 Terms and Conditions of Employment

Legly will state the employee's roles and responsibilities for information security in the terms and conditions of employment.

The purpose of this policy is to make clear to all employees their responsibilities for maintaining and promoting security within the organization during and subsequent to their employments as well as the sanctions for not doing so.

The employee's manager will provide the employee specific responsibilities that are particular to the specific position.

Disciplinary measures are covered in section 6.3.4 of this policy.

6.2 Employee Training

All employees will be appropriately trained on the organization's Information Security policies and kept up-to-date on any additions or changes to the policies. Training is mandatory prior to receiving access to information or services.

Management is responsible for initial training and education on the organization's security policies during the employee orientation process. Employees should have recurring annual refresher training on current threats, as well as material changes to policy. This training may be conducted by annual refresher seminars or continual reminders (such as posters, e-mail or intranet newsletters, etc.).

When employees sign acknowledgements for complying with policy, these acknowledgements should include acknowledgement of initial training.

Management will be responsible for the on-going policy education and training policy.

6.3 Responding to Security Incidents

6.3.1 Reporting Security Incidents

Legly will educate employees on and establish formal reporting and feedback procedures and incidence response procedures for all security incidents. In this way, we will react to all security incidents immediately and providing all employees with the information necessary to assist the organization is doing so immediately.

All suspected policy violations, system intrusions, virus infestations and other conditions that might jeopardize Legly information or Legly information systems shall be immediately reported.

If an employee learns that Legly confidential information has been lost, disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the employee shall immediately notify management.

See 10.0 for more information.

6.3.2 Reporting Security Weaknesses

We require all users to immediately report suspected security weaknesses in, or threats to, systems or services to management or service providers.

6.3.3 Learning from Incidents

The purpose of this policy is to allow the organization to enhance the organization's security policy to limit such occurrences in the future.

Incidents and malfunctions will be reviewed during the security review process (see 3.1). Analysis of incidents and malfunctions will be done to determine new controls that can be established to prevent future incidents.

6.3.4 Disciplinary Process

In support of the Information Security Program, we will establish a disciplinary process for those who violate the organization's security policies and procedures.

If an employee is suspected of a breach of security, management shall be informed and shall begin the investigation.

7.0 VULNERABILITY MANAGEMENT

Effective vulnerability management can reduce risk to Legly's computing environment by verifying that systems or network devices are using current patch levels, are not running unnecessary services, and do not have default passwords.

Legly shall run internal vulnerability scans against any systems containing (or accessing systems that contain) confidential data at least on a quarterly basis.

Legly shall contract with a trusted third party to run external vulnerability scans and penetration tests against the Legly service on at least an annual basis.

7.1 Protection Against Malicious Software

Legly shall implement procedures, user awareness, and change controls to detect and prevent the introduction of malicious software into the organization's computing environment. This policy will protect the integrity of software and information by promoting procedures and user actions to mitigate the risks of the introduction of malicious software into the organization.

To prevent interrupted service caused by computer viruses for both computers and networks, all personal computer users must keep current versions of approved virus-screening software enabled on their primary computers at all times.

7.2 Information Backup

We will regularly back-up adequate copies and generations of all software, documentation and customer data. Regular testing will be done to ensure the quality and usability of backed-up resources. The purpose of this policy is to maintain the availability and integrity of information resources in the case of failure or disaster, by retaining up-to-date back-ups that are stored at a distance sufficient to escape damages that might occur at the main site.

Restoration procedures will be documented and tested to ensure that they are effective and comply with restoration time requirements.

Back-up media shall be tested semi-annually to ensure the back-up can be relied upon. IT shall be responsible for ensuring that back-ups are tested.

Retention schedules will be adhered to for all business information.

8.0 ACCESS CONTROL

We will define and document access control rights and rules for each employee. Service providers shall be given clear statements of the business requirements met by these access controls. Access to information and information services will only be given on the basis of business and security requirements.

The guiding principle is that access will be given on a need-to-know basis, based upon the security requirements and business requirements of individual business applications. Access to information shall be provided in a manner that aims to protect the confidentiality and integrity of that information and without compromise to associated information or raw data. Access control rights should be reviewed regularly to ensure that all access rights are authorized and remain appropriate, and that no unauthorized privileges have been gained.

Access will be given that is consistent with security levels and classifications, consistent with legislation and contractual obligations for confidentiality.

Administrator access to production systems will be limited to only those with a justified business requirement for such access. Developers and other application personnel will not have access to the underlying operating system on production systems, unless necessary.

Each defined asset (see 5.0) has its own set of access control levels and an employee will be given access based on a Least-Privileged basis, so that they are limited to only those functions their work requires them to be.

8.1 Employee Access Management

A registration and deregistration process must be used for gaining access to various Legly systems. This process must protect and maintain the security of access to the organization's information resources through the complete life cycle of the user.

The level of access for the employee will be determined by management and recorded. System owners and/or management shall grant access rights for each asset as needed.

Access rights shall immediately be removed or modified when an employee leaves the company or changes jobs.

8.1.1 Authentication & Authorization

The account and password are the primary means of verifying an employee's identity. The allocation of passwords might be a formal management process, otherwise they should adhere to our Password Policy (see …).

Employees will be responsible for the secure storage of their passwords.

Passwords will be given in a secure manner (i.e. not in a plain text e-mail).

Multi-factor login should be used whenever possible.

8.1.2 Review of Access Rights

Access rights will be reviewed at regular intervals. Management will review their employee's rights to ensure they are consistent with their present job function. IT will review user rights to ensure that elevated privileges have not been granted out without authorization, and that accounts that have not been used recently or belong to terminated employees are deactivated or purged.

8.2 Employee Responsibilities

8.2.1 Password Use

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Legly's entire corporate network. As such, all Legly employees (including contractors and vendors with access to Legly systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Legly facility, has access to a Legly network or service, or stores any non-public Legly information.

8.2.1.1 User Password Rules

All users will keep their passwords confidential and store them securely.

Users will be made aware of good security practices and the requirement to use good security practices with their passwords.

All passwords are to be treated as confidential Legly information. They should not be shared with anyone, including administrative assistants.

Password requirements:

- Passwords will be at least 8 characters long.
- Passwords will be composed of alpha-numeric characters.
- Passwords will contain a mix of upper case and lower case, numbers and non-alpha-numeric characters.

8.2.2 Unattended User Equipment

Users shall protect Legly's information resources from unauthorized access by protecting unattended equipment:

- Users will terminate active sessions when finished (or unattended) or secure by appropriate locking functions.
- Users will log off of multi-user systems when finished.
- Users will log off or lock terminals when unattended.
- PCs or terminals shall be locked (i.e. by a key or password) when not in use.
- A password-protected screen saver will be automatically invoked after 20 minutes of inactivity.

8.3 Sensitive Assets

Highly sensitive systems will have network access controls (i.e., firewalls or IP whitelists) in place to prevent unauthorized connections from inside, or outside, Legly. This is in addition to any application or system access controls. Restrictions will be consistent with the access control policy.

An annual risk assessment will be performed to establish which systems and/or applications should be protected.

8.4 Monitoring & Logging Access

We will monitor the use of information processing facilities to detect unauthorized activities and ensure that users and services are only performing the functions and gaining access to information to which they are authorized.

Each service, system or application shall be risk-assessed to determine the level of monitoring required. Extra care should be given to monitoring system exceptions or failures, privileged/unauthorized access attempts and access to customer data.

Event logs will contain:

- Identity of the user, service or system used to authenticate
- Identity of the service, system or application where the event occurred
- Timestamp
- Information about the request and whether it was successful

9.0 INCIDENT RESPONSE

Security incidents must be reported promptly to Legly's developers and system administrators.

This document establishes the procedures for identifying, reporting and responding to an information security event. It also identifies roles and responsibilities involved in responding to and recovering from these events.

The objectives of the Incident Response Plan are to:

- Enable Legly to respond to an information security incident without delay and in a controlled manner
- Enable assessment of mitigation measures that can be taken to protect information, assets, customer data and privacy and limit or prevent damage during an active incident
- Ensure provision of timely notification of those who need to know, including but not limited to management and customers
- Continuously improve and learn from information security events

9.1 Scope

The Incident Response Plan should be followed when the following types of events occur:

- Any unauthorized access to data, resources or systems owned and/or controlled by Legly
- Any such incident involving an employee of Legly
- Any such incident involving third party providers, such as cloud services or authentication/authorization services

9.2 Incident Reporting

Information security incidents are events that have the potential compromise the confidentiality, integrity or availability of Legly's information and/or information technology resources.

Use the #security channel on Legly's Slack workspace to report any potential information security incident to developers and system administrators. Make sure they confirm they have seen and understood your notification.

Examples of Information Security Incidents

- Account(s) accessed by an unauthorized person
- Compromised and/or leaked
- Device(s) infected with malware or ransomware
- Unintentional or intentional disclosure of protected Legly data to an unauthorized person or people
- Unauthorized access to, alteration of, or activity within one of Legly's information systems (unexplained or unauthorized code changes, compromised/defaced website, etc.)
- Stolen or lost laptop, tablet computer or smartphone
- Denial of Service Attack
- Third-party services and providers notifying us of an information security incident of their own

9.3 Incident Response

Once an incident has been reported to the developers and system administrators they will serve as the primary point of contact and coordination for the duration of the incident.

9.3.1 Step 1: Assign Point of Contact & Incident Coordinator

When an incident has been reported and determined to not be a false alarm, a member of the developer or system administrator team will be assigned as the primary point of contact and incident coordinator for the duration of the response and recovery effort. Use the #security channel on Legly's Slack workspace as the main communications channel concerning the incident.

9.3.2 Step 2: Incident Identification & Threat Classification

The incident coordinator and their team review the known details of the incident and determine the incident's initial risk classification. Use the data classification matrix to gauge how critical the incident is by estimating its consequences and the kind of data at risk.

Important questions to address

- When did the event happen?
- How was it discovered?
- Who discovered it?
- Have any other areas been impacted?
- What is the scope of the compromise?
- Does it affect operations?
- Has the source (point of entry) of the event been discovered?
- What data is at risk?
- Is it an ongoing event?

9.3.3 Step 3: Containment & Mitigation

If the incident is ongoing it is imperative that systems, services and data are protected and secured against further disruptions and breaches. Strategies for this should be discussed and implemented as soon as possible and may include (but are not limited to):

- Firewall ports may need to be blocked until the source of an attack is known
- Systems may need to be shut down or taken off-line until they can be protected without disrupting services
- Protocols may need to be disabled temporarily
- Access to all users, storage, applications, subnets, etc. may need to be disabled until the extent of any compromise is understood
- Network access may need to be blocked or restricted to prevent additional intrusion or the spread of malware

Important questions to address

- What has been done to contain the breach short term?
- What has been done to contain the breach long term?
- Has any discovered malware been quarantined from the rest of the environment?
- What sort of backups are in place?
- Does your remote access require true multi-factor authentication?
- Have all access credentials been reviewed for legitimacy, hardened and changed?
- Have you applied all recent security patches and updates?

9.3.4 Step 4: Investigation & Eradication

With the breach contained it is time to find and eliminate the root cause of the incident. This means malware need to be securely and thoroughly removed and all exploits patched. Learn as much as needed about the technical aspect of the incident to feel confident in that the cause of the incident has been neutralized and taken care of.
Do not rush this stage. It is important to make sure no traces of malware or usable security exploits persist, lest valuable data is still put at risk.

Important questions to address

- Have artifacts/malware from the attacker been securely removed?
- Have used exploits been identified and patched?
- Has the source (point of entry) of the event been discovered?
- Which systems have been affected?
    - Did the incident result in the exposure or potential exposure of restricted data?
    - Did the incident involve criminal activity?

9.3.5 Step 5: Recovery

After the incident has been investigated and the damage contained and neutralized it is important to get your systems and business operations up and running again. The actions needed to accomplish this will vary depending on the type and scale of the incident and may include:

- Patching vulnerabilities in the impacted infrastructure components and identifying similar infrastructure components that might share that vulnerability in order to apply preventive patches
- Securing the accounts of compromised users
- Rolling back application code to pre-compromise backups
- Implementing additional security controls on impacted devices, systems, or networks
- Improving business processes to reduce the risk of recurrence
- Revising policies and procedures to reduce the risk of recurrence or the impact from similar future incidents
- Documenting the acceptance of risk in situations where the vulnerability or circumstance that enabled the incident to occur cannot be mitigated or remediated

Important questions to address

- When can systems be returned to production?
- Have systems been patched, hardened and tested?
- Can the system be restored from a trusted back-up?
- How long will the affected systems be monitored and what will you look for when monitoring?
- What tools will ensure similar attacks will not reoccur? (File integrity monitoring, intrusion detection/protection, etc.)
- What should be communicated to users and customers?

-

9.3.6 Step 6: Lessons Learned

All incidents should be analyzed and discussed, but those that have been deemed major or critical (concerning sensitive or protected data as defined by the data classification matrix) need to be taken extra seriously. Documentation on the incident, how it was dealt with and what changes need to be done going forward should be compiled.

Important questions to address

- What changes need to be made to the security?
- How should employees be trained differently?
- What weakness did the breach exploit?
- How will you ensure a similar breach does not happen again?
- What did and did not work in the incident response plan?

10.0 REVIEW & COMPLIANCE

To maintain the security, integrity and availability of the organization's information processing assets, we will continually monitor the company's compliance with its security policies.

Management shall ensure that an annual internal audit takes place. The scope of this audit is a security assessment for all listed assets and a sweep for potential unlisted assets, as well as general employee compliance and knowledge of relevant security policies.

We shall also contract with a trusted third party to run external vulnerability scans and penetration tests against the Legly service on at least an annual basis.