**EXECUTIVE SUMMARY**

To maintain the trust of our employees, customers, and partners and meet regulatory requirements, it is essential that we do everything we can to protect confidential information and systems in the face of a cyberattack. The better prepared we are to respond to a potential cyberattack, the faster we can eradicate any threat and reduce the impact on our business.

This document describes the plan for responding to information security incidents at LearnIt. This document will explain how to detect and react to cybersecurity incidents and data breaches, determine their scope and risk, respond appropriately and quickly, and communicate the results and risks to all stakeholders.

Effective incident response involves every part of our organization, including IT teams, legal, technical support, human resources, corporate communications, and business operations. It is important that you read and understand your role as well as the ways you will coordinate with others.

This plan will be updated *once annually* to reflect organizational changes, new technologies and new compliance requirements that inform our cybersecurity strategy. We will conduct regular testing of this plan to ensure everyone is fully trained to participate in effective incident response.

Contents

[Incident Response Team Responsibilities 3](#_Toc100306690)

[Roles, Responsibilities, and Contact Information 3](#_Toc100306691)

[Testing and Updates 4](#_Toc100306692)

[INCIDENT RESPONSE PROCESS OVERVIEW 5](#_Toc100306693)

[Incident Response Checklist 5](#_Toc100306694)

[Document Control 9](#_Toc100306695)

**ROLES, RESPONSIBILITIES & CONTACT INFORMATION**

This Security Incident Response Plan must be followed by all personnel, including all employees, temporary staff, consultants, contractors, suppliers, and third parties operating on behalf of *LearnIt.* All personnel are referred to as ‘staff’ within this plan.

Below are details about the roles and responsibilities of each member of LearnIt to prevent and respond to a workplace incident. It is not an exhaustive list of duties but is designed to give each employee a general understanding of their role and the roles of other employees in incident response and prevention.

# Incident Response Team Responsibilities

The Security Lead is responsible for:

* Making sure that the Security Incident Response Plan and associated response and escalation procedures are defined and documented. This is to ensure that the handling of security incidents is timely and effective.
* Making sure that the Security Incident Response Plan is current, reviewed, and tested at least once each year.
* Making sure that staff with Security Incident Response Plan responsibilities are properly trained at least once each year.
* Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Response Plan when needed.
* Reporting to and liaising with external parties, including pertinent business partners, legal representation, law enforcement, etc., as required.
* Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from the site.

All staff members are responsible for:

* Making sure they understand how to identify and report a suspected or actual security incident.
* Reporting a suspected or actual security incident to the Incident Response Lead.
* Reporting any security-related issues or concerns to line management, or to a member of the SIRT.
* Complying with the security policies and procedures of LearnIt.

# Roles, Responsibilities, and Contact Information

|  |  |  |
| --- | --- | --- |
| ROLE | RESPONSIBILITY | CONTACT DETAILS |
| **INFORMATION SECURITY** | | |
| **Security Lead** | * Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plans. * Authorizes when and how incident details are reported. * Maintains incident response plan, documentation, and catalog of incidents. * Responsible for identifying, confirming, and evaluating the extent of incidents. * Conducts random security checks to ensure readiness to respond to a cyberattack. | Name: Hunter Schattie  Email: HS49@students.uwf.edu |
| **SOFTWARE DEVELOPMENT** | | |
| **Code / Testing / Software Engineering Leads** | * Work with security lead to mitigate software vulnerabilities. * Provide information or data needed for investigation | Name: Brandon Kelley  Email: BMK24@ students.uwf.edu  Name: Serghei Berezovschi  Email: SB206@ students.uwf.edu |

# Testing and Updates

Annual testing of the Incident Response Plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure the Security lead is aware of their obligations unless real incidents occur that test the full functionality of the process.

1. The Incident Response Plan will be tested at least once annually.
2. The Incident Response Plan Testing will test LearnIt’s response to potential incident scenarios to identify process gaps and improvement areas.
3. The Security Lead will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.
4. The Security Lead will ensure the Security Incident Response Plan is updated and distributed to SIRT members.

# INCIDENT RESPONSE PROCESS OVERVIEW

Below is the structured 6-step process followed in this document as defined by the SANS Institute in their [Incident Handler’s Handbook](https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901). The six steps outlined are:

1. **Preparation**—review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Computer Security Incident Response Team (CSIRT).
2. **Identification**—monitor IT systems and detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.
3. **Containment**—perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production while rebuilding clean systems.
4. **Eradication**—remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.
5. **Recovery**—bring affected production systems back online carefully, to prevent additional attacks. Test, verify, and monitor affected systems to ensure they are back to normal activity.
6. **Lessons learned**—no later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, and understand what was done to contain it and whether anything in the incident response process could be improved.

# Incident Response Checklist

To demonstrate and improve the effectiveness of Learnit incident response team and security tools, LearnIt requires a record of all actions taken during each phase of an incident. Supporting documentation is required, including all forensic evidence collected such as activity logs, memory dumps, audits, network traffic, and disk images.

|  |  |  |  |
| --- | --- | --- | --- |
| PHASE OF CYBER INCIDENT | ACTION | TEAM MEMBER/ SYSTEM | DAY/TIME  ACTION TAKEN |
| **Incident Discovery and Confirmation** | Describe how the team first learned of the attack (security researcher, partner, employee, customer, auditor, internal security alert, etc.). |  |  |
| Analyze audit logs and security applications to identify unusual or suspicious account behavior or activities that indicate a likely attack and confirm attack has occurred. |  |  |
| Describe potential attacker, including known or expected capabilities, behaviors, and motivations. |  |  |
| Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party. |  |  |
| Prepare an incident timeline to keep an ongoing record of when the attack occurred and subsequent milestones in analysis and response. |  |  |
| Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites. |  |  |
| Evaluate extent of damage upon discovery and risk to systems and privileged accounts. Audit which privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed. (See Appendix A for more information on Threat Classification). |  |  |
| Review your information assets list to identify which assets have been potentially compromised. Note integrity of assets and evidence gathered. (See Appendix A for more information on Threat Classification). |  |  |
| Diagram the path of the incident/attack to provide an “at-a-glance” view from the initial breach to escalation and movement tracked across the network. |  |  |
| Collect meeting notes in a central repository to use in preparing communications with stakeholders. |  |  |
| Inform employees regarding discovery. |  |  |
| Analyze incident Indicators of Compromise (IOCs) with threat intelligence tools. |  |  |
| Potentially share information externally about breach discovery. You may choose to hold communications during this phase until you have contained the breach to increase your chances of catching the attacker. If so, make sure this aligns with your compliance requirements. |  |  |
| **Containment and Continuity** | Enable temporary privileged accounts to be used by the technical and security team to quickly access and monitor systems. |  |  |
| Protect evidence. Back up any compromised systems as soon as possible, prior to performing any actions that could affect data integrity on the original media. |  |  |
| Force multi-factor authentication or peer review to ensure privileges are being used appropriately. |  |  |
| Change passwords for all users, service, application, and network accounts. |  |  |
| Increase the sensitivity of application security controls (allowing, denying, and restricting) to prevent malicious malware from being distributed by the attacker. |  |  |
|  | Remove systems from production or take systems offline if needed. |  |  |
| Inform employees regarding breach containment. |  |  |
| Analyze, record, and confirm any instances of potential data exfiltration occurrences across the network. |  |  |
| Potentially share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.). |  |  |
| **Eradication** | Close firewall ports and network connections. |  |  |
| Test devices and applications to be sure any malicious code is removed. |  |  |
| Compare data before and after the incident to ensure systems are reset properly. |  |  |
| Inform employees regarding eradication. |  |  |
| Potentially share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.). |  |  |
| **Recovery** | Download and apply security patches. |  |  |
| Close network access and reset passwords. |  |  |
| Conduct vulnerability analysis. |  |  |
| Return any systems that were taken offline to production. |  |  |
| Inform employees regarding recovery. |  |  |
| Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.). |  |  |
| **Lessons Learned** | Review forensic evidence collected. |  |  |
| Assess incident cost. |  |  |
| Write an Executive Summary of the incident. |  |  |
| Report to executive team and auditors if necessary. |  |  |
| Implement additional training for everyone involved in incident response and all employees. |  |  |
| Update incident response plan. |  |  |
| Inform employees regarding lessons learned, additional training, etc. |  |  |
|  | Potentially share information externally (website updates, emails, social media posts, tech support bulletins, etc.). |  |  |

# Document Control

|  |  |
| --- | --- |
| Document Name: | Security Incident Response Plan |
| Current Version: 1 |  |
| Plan Owner: LearnIt |  |
| Plan Approver: Hunter Schattie |  |
| Date of Last Review: | 4/8/2022 |