	SOP #:	IT-1001
	Revision #:	2.0
	Implementation Date:	02/01/2023
Page 1 of 9		Last Reviewed/Update Date: 03/30/2023
SOP Owner:	Ken Barbie	Approval: [PERSON]


INFORMATION TECHNOLOGY & SECURITY

Incident Response Plan

Purpose

The purpose of this response plan is for Acme Learning Partners (ALP) to classify, declare, escalate, respond, and contain any cybersecurity events that occur. These are ones that are considered harmful to the company, our partners, vendors, patients, and/or employees. To minimize impact to all, we have created this document to aid in classifying any incoming events that result in a reduction or disruption of normal business activities.

Disclaimer

	<p>WARNING</p> <p>Information contained in this section is proprietary and is exclusive to ALP and customers or clients that have an active or pending contract or Statement of Work (SOW) in place. Under any circumstances do not share the details of the action plan with the public or others externally without written permission from Executive Leadership.</p>
-----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Scope


This document establishes the recommended organization, actions, and procedures needed to do the following tasks:

- ✓ Recognize and respond to an incident
- ✓ Assess the situation quickly and effectively
- ✓ Notify the appropriate individuals and organizations about the incident
- ✓ Organize ALP's response activities
- ✓ Escalate ALP's response efforts based on the severity of the incident
- ✓ Support the business recovery efforts being made in the aftermath of the incident

As provided here, these are in place in an attempt to eliminate or at the minimum reduce the operational and financial impacts of such an incident. The actions in this plan are activated whether a Technology Manager (or in their absence, a designated alternate contact) determines that an incident has occurred.

Training

This document applies to all ALP Information Technology employees, managers, and consultants. It also applies to ALP employees or consultants identified as Business Owner (BO) of specified ALP business applications due to its importance to the organization. Other personnel, such as stakeholders and/or client/customer contacts may be included when business needs necessitate or require as part of a formal agreement.

	SOP #:	IT-1001
	Revision #:	2.0
	Implementation Date:	02/01/2023
Page 2 of 9	Last Reviewed/Update Date:	03/30/2023
SOP Owner: Ken Barbie	Approval:	[PERSON]

Incident Response Plan Process and Detail

The Incident Response Plan (going forward known as the IRP) is made up of four (4) levels that escalated from the previous one(s) shared. Depending on the incident, it may bypass specific levels depending on the severity or impact to the organization. To begin, here is a visual outlay of the levels:

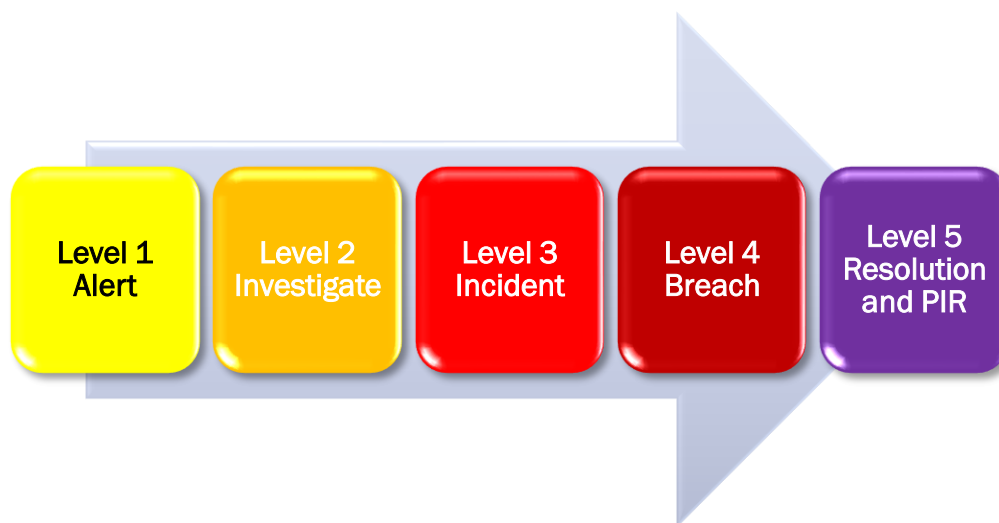



Figure 1 – IRP Severity Index (Level 1 = Lowest; Level 4 = Highest)

	<p>NOTE</p> <p>The IRP Severity Index is NOT a cyclical process. Depending on the type of incident, it may be resolved at any one of the levels or be escalated to the highest level shown. Each alert provided is independent to others that have already been diagnosed and resolved.</p>
-------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Level 1 – Alert


The initial security notification is an alert. It is a documented event that needs to be reviewed. To best determine what has occurred, an investigation must take place. Cybersecurity events that could be harmful, violate security policies, or require an escalation to a higher level are documented initially in the form of an alert. Common sources of alerts may come from the following resources:

- ✓ End users which include employees, system users, or customer/client users that have access to select ALP systems as part of their work tasks and/or duties
- ✓ Security Management Consoles (such as endpoint protection or firewalls).
- ✓ Managed Security Partners
- ✓ Government & Law Enforcement
- ✓ Customers or clients that may have been exposed themselves

Alerts can be brought to the attention of the Technology Support and Security teams in the form of an email, phone call, chat, or direct walk up.

Level 2 – Investigation

An investigation is an effort to learn further information about alerts identified so that it can be determined if one has occurred. It can also determine if it can be resolved without further interventions or resources. This set

	SOP #:	IT-1001
	Revision #:	2.0
	Implementation Date:	02/01/2023
Page 3 of 9		Last Reviewed/Update Date: 03/30/2023
SOP Owner:	Ken Barbie	Approval: [PERSON]

of actions and sources of additional information will be determined by the security resource working the primary investigation. At this point in time, no formal communication is required to take place while the investigation takes place.

An alert that was reported that has successfully reviewed with no additional actions required will be closed and resolved. In the event the investigation has resulted in an unfavorable outcome for the company, the client/customers impacted, systems, or other targets, it will escalate further to the next level.

Level 3 – Incident

Upon conclusion of the **initial** investigation conducted in Level 2 of the IRP, it is possible that further action is required. If results show that there has been some impact to the company, clients or customers, systems, or others, the alert is then escalated to this level. As a result, the investigation continues because of evidence noting that malicious activity, policy violation, data loss, or other tangible or intangible losses have occurred. Thus, the primary resource performing the incident handling should communicate an incident to the director of IT, and the lead cybersecurity resource (if different).

Documentation should begin as part of the incident handling and include, when possible, the following:


- ✓ The source of alerts which initiated an investigation
- ✓ Time and date of incident(s) and resources supporting incident
 - ❖ **Time to detect:** To the best of the ability at such time, when the origin of the incident began to the time the someone started investigating the alerts (not the alert origination)
 - ❖ **Time to respond:** The amount of time between when the incident began and the time the formal incident declaration has begun
 - ❖ **Time to contain:** The amount of time between when the incident was identified, and the time containment of incident was successful
 - ❖ **Time to remediate:** Measurement of time between incident actually began and the time to bring impacted assets back to operational status
- ✓ All applicable evidence collected so that there is support in the event a prosecution is required per guidance from authorities, our customers and/or clients as well as Executive Leadership where appropriate
- ✓ Documented chain of custody of all evidence which is held in a secure location online and offline (where applicable or relevant)

Refer to [Form ITF-1002 – System Incident Report \(FORM-IncidentReport.docx\)](#) for information on how to record a cybersecurity incident in the Cybersecurity SharePoint Folder.

Level 4 – Breach

A breach is declared when there is evidence or valid reasoning to believe that a data loss has occurred at ALP, or other compromises of data or systems have occurred at ALP. In most cases, these are formally declared by the resource(s) handling the incident as well as at least one other primary management resource (Head of IT, CFO, or CEO). The handling of the cybersecurity breach will be handled in accordance with the information furnished in the [Level 3 – Incident](#) analysis. Any attempted breach may be raised to this level depending on the impact and severity of the attack that took place.

Primary actions of a breach are focused on the escalation and communication of the cybersecurity event that took place. The level of the cybersecurity event should be declared by the designated cybersecurity resource. This can either be security staff, technology staff designated with security responsibilities assigned by management, technology directory, or the managed security service partner.

	SOP #:	IT-1001
	Revision #:	2.0
	Implementation Date:	02/01/2023
Page 4 of 9		Last Reviewed/Update Date: 03/30/2023
SOP Owner:	Ken Barbie	Approval: [PERSON]

Level 5 – Resolution and Post Incident Reviews (PIRs)

Once a breach has been declared, it is important to resolve it as urgently as possible. This is to ensure that minimal damage has been done to any party that is affected tangibly or intangibly from the incident. All SIRT personnel must work together to complete this task in a timely manner. Once the breach and/or incident has been successfully completed, a summary of the incident and resulting outcome should be documented. This is a preventative measure should the same breach occur again and be mitigated sooner in the process.

To minimize the impact on the business, our customers, clients, and contractors, we will offensively and proactively locate the source and deprovision the system(s) that were concluded to be the result of the investigation. Since we do not handle any information physically on-site, we will reprovision that instance and rebuild the system(s) affected in a timely manner. All data that was on the instance or systems that were negatively impacted are erased and permanently lost.

Post Incident Reviews (or PIRs) should also be prepared to analyze the handling and successful resolution of the attack that took place. If needed, public statements may need to be made as part of the PIR. This is to preserve the brand image of not only ALP but the customers and clients that were negatively affected. Executive Leadership is recommended to meet no more than five (5) business days once resolved to discuss. Otherwise, if not applicable, the SIRT team disbands and returns to their normal duties and work tasks and the process completes.


Resources

Upon declaration of an incident, the security resource will communicate to the Director of Technology, Head of IT, or other equivalent stakeholder. This may also include contacting the client/customer's main point of contact (e.g. Hasbro) if their information is compromised as a result internally or otherwise. These resources are in place to contain, remediate, respond, and recover from an incident as quickly as possible. Personnel that are grouped together utilizing their skills and knowledge for this purpose are referred to as the **Security Incident Response Team (SIRT)**.

If you are asked to participate on a SIRT, please contact your direct manager or leader to prioritize tasks for this team above and beyond work that is already in progress internally and/or externally. Once approval has been authorized, full focus must be on rectifying all incidents and/or breaches that are active or outstanding.

Incident Documentation

It is very important to document all information relevant to cybersecurity incidents. As such, once an event is classified as an incident (or Level 3, it should be recorded and all evidence relevant to the event should be saved and archived to the best of the ability of the staff and support involved. Evidence of cyberattacks are documented and retained because in the event ALP decides to pursue legal action, evidence will be required as part of the case. Evidence collection should follow security best practice and have chain of custody log kept if, and when evidence is moved, changes ownership, stored on external media, or transfer to other organizations.

	SOP #:	IT-1001
	Revision #:	2.0
	Implementation Date:	02/01/2023
Page 5 of 9		Last Reviewed/Update Date: 03/30/2023
SOP Owner:	Ken Barbie	Approval: [PERSON]

Incident Documentation

The following escalation guidelines provide directions on when staff, partners, legal teams, and regulatory bodies should be notified as a part of ALP's incident response plan.

- ✓ **Alerts & Investigations:** These events will be recorded within security consultations, and maybe documented separately for investigations justifying further documentation and tracking. Clients or customers may also be required to be notified depending on the nature of the attack or breach.
- ✓ **Incidents:** The head of the IT department should be notified that a cybersecurity incident has been opened and is being worked on without exception.
- ✓ **Breach:** In the event a breach occurs, immediate escalation should be communicated to the Executive Leadership team as determined by the head of the IT department, compliance resources, internal and/or external legal resources, and privacy resources when appropriate. The client should also be immediately notified if their systems and/or data is the focus of the breach.

Executive Breach Notification Requirements

A cybersecurity breach requires escalation and communication to an executive leader resource. At such a point, the executive resource is made aware of the situation they will make the decision if further escalation and combination needs to take place. This may include HR, Legal, Privacy, Compliance, Public Relations. This effort should take place quickly enough so that proper escalation to law enforcement and regulatory agencies can take place within the required guidelines. Refer to Section 2 of [Form ITF-1002 – System Incident Report \(FORM-IncidentReport.docx\)](#) in the Cybersecurity SharePoint Folder for additional information.

Post-Incident Reviews (PIRs)

A review of the cybersecurity incident should be performed within **three (3) business days** of the incident for more than one compromised system because of an attack or no more than **five (5) business days** for less severe incidents. All team members involved in the triage, classification, investigation, containment, and resolution of the event should be involved. The purpose of this review is to clarify lessons learned to:


- ✓ Prevent the same incident from happening again
- ✓ Speed up the containment of the incident
- ✓ Improve escalation and team response and handling
- ✓ Decrease the time of resolution and recovery

Roles and Responsibilities

The information contained in this section provides general guidelines and responsibilities for persons that identify the incident and/or part of the SIRT. They are as follows:

Incident Response Lead

- ✓ Making sure that your Incident Response Plan and Incident response procedures are defined and documented. This is to make sure that the handling of security incidents is timely and effective.
- ✓ Ensure that the Incident Response Plan is up to date, reviewed and tested, at least once each year.
- ✓ Verify that staff with Incident Response Plan responsibilities are properly trained.
- ✓ Lead the investigation of a suspected breach or reported security incident and initiating the Incident Response Plan, as and when needed.
- ✓ Report to and liaising with external parties.
- ✓ Preserve evidence during incident. This will be shared with the SIRT members.

	SOP #:	IT-1001
	Revision #:	2.0
	Implementation Date:	02/01/2023
Page 6 of 9		Last Reviewed/Update Date: 03/30/2023
SOP Owner:	Ken Barbie	Approval: [PERSON]

- ✓ Authorize on-site investigations by appropriate law enforcement or security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.

Security Incident Response Team (SIRT) Members

- ✓ Understand how to identify and report a suspected or actual security incident.
- ✓ Advise the Incident Response Lead of an incident when they receive a security incident report from staff.
- ✓ Comprehend incident procedures and ability to carry out the response.
- ✓ Investigate and validate each reported incident.
- ✓ Take action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- ✓ Gather, review, and analyze logs and related information from various central and local safeguards, security measures and controls.
- ✓ Document and maintain accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- ✓ Report each security incident and findings to the appropriate parties. This may include the acquirer, third party service providers, business partners, customers, etc., as required.
- ✓ Assist and cooperate with law enforcement and security personnel during the investigation processes. This includes any forensic investigations and prosecutions.
- ✓ Resolve each incident to the satisfaction of all parties involved, including external parties.
- ✓ Initiate follow-up actions to reduce likelihood of recurrence, as appropriate.
- ✓ Be held responsible for understanding and following through on preservation of evidence and data.
- ✓ Determine if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future.
- ✓ Conclude whether additional safeguards are required in the environment where the incident occurred.

ALP Staff Members


- ✓ Learn and accurately identify a suspected or actual security incident when it occurs.
- ✓ Report a suspected or actual security incident to the Incident Response Lead (preferably) or to another member of the SIRT no more than 24 hours from the time it was discovered.
- ✓ Comply with all security policies and procedures outlined by ALP.

Communication Escalation Matrix


The matrix on the next page attempts to define who should be communicated to in the event of an incident or a breach. The event declarations drive the communication levels indicated below and the role responsible for that communication path. This also attempts to identify the escalation 'path', meaning who should be responsible for escalating to the next level. (i.e., IT Director will escalate to General Counsel, who will escalate to Public Relations, who will in turn inform the Public). Do note that the customer or client should be communicated to as early as possible in the process regardless of the severity level outlined in this procedure.

Please note that the final level, [Level 5 - Resolution and Post Incident Reviews \(PIRs\)](#) is specifically internal and is to close out a breach that has been detected and rectified.

(Continues on the next page)


	SOP #:	IT-1001
	Revision #:	2.0
	Implementation Date:	02/01/2023
Page 7 of 9		Last Reviewed/Update Date: 03/30/2023
SOP Owner:	Ken Barbie	Approval: PERSON

	Levels of the Incident Response Plan			
Event	Level 1	Level 2	Level 3	Level 4
Alert	IT Resource Lead			
Investigation	IT Resource Lead	IT Resource Lead & Head of IT		
Incident(s)	IT Resource Lead & Head of IT	IT Resource Lead & Head of IT	IT Resource Lead, Head of IT, & CEO	
Breach(es)	IT Resource Lead & Head of IT	IT Resource Lead & Head of IT	IT Resource Lead, Head of IT, Public Relations, Legal Partner, Executive Leadership, & CEO	IT Resource Lead, Head of IT, Public Relations, Legal Partner, CEO, Executive Leadership, Employees, and General Public (when necessary)

	<p>NOTE</p> <p>Depending on the severity of the issue at hand, it is at the discretion of the IT Resource Leader to determine additional parties that may be included. This may include client/customer contacts where appropriate and necessary.</p>
-----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Roles and Responsibilities


Role	Current Personnel	Responsibilities
Executive Committee	G. I. Joseph, CEO <u>Email: joe@Acmelearning.com</u> <u>Mobile: (555) 555-1234</u>	Senior Management is responsible for ensuring that they are briefed by the Head of IT, at least annually, on the effectiveness of this Policy.
Incident Response Team	Ken Barbie, Head of IT <u>ken@Acmelearning.com</u> Mobile: (555) 555-2345 Barbie Ken, IT Specialist, <u>barbie@Acmelearning.com</u> Mobile: (555) 555-3456	<p>The Head of IT is responsible for the overall compliance with this Incident Response Plan. Under its direction and support, ALP will be directed to implement and maintain this plan. They also will use his/her discretion to notify the CFO and General Counsel of Information Incidents to assess whether escalation to the Senior Management team is necessary.</p> <p>The ALP Incident Response team is responsible for responding to Information Incidents. The escalation path for each division responding to incidents is first IT, next level is Assistant General Counsel, and the final level is General Counsel.</p>
Board of Directors and General Counsel	Contact Information on file.	The ALP Board of Directors is responsible for supporting the IR strategy and execution. The Board is responsible for ensuring that it receives periodic updates regarding ALP's cybersecurity risks.

	SOP #:	IT-1001
	Revision #:	2.0
	Implementation Date:	02/01/2023
Page 8 of 9	Last Reviewed/Update Date:	03/30/2023
SOP Owner: Ken Barbie	Approval:	[PERSON]

Document References

The following pieces of information were derived from the following linked resources:

- ✓ [Microsoft Defender Vulnerability Management](#)
- ✓ [Microsoft Internal Security Risk Detection](#)
- ✓ [Microsoft Security Development Lifecycle \(SDL\)](#)
- ✓ [Remote Workforce Security Management](#)
- ✓ [Threat Management Overview](#)
- ✓ [Vulnerability Management](#)

	SOP #:	IT-1001
	Revision #:	2.0
	Implementation Date:	02/01/2023
Page 9 of 9		Last Reviewed/Update Date: 03/30/2023
SOP Owner:	Ken Barbie	Approval: [PERSON]

Revision History

The following is the content change control history for this procedure:

Date	Version	Change(s) Applied	Personnel Applying Change(s)
02/01/2023	1.0	Initial Creation of Document	Ken Barbie
03/30/2023	2.0	Major Modifications to Document; Grammar and Spelling Adjustments; Updated Content To Reflect Intended Audience; Added Customer/Client Focus for Emphasis on Clear Communication When Security Issues Occur	Doug Trovinger