ULT Cyber Incident Response Plan

UTTOXETER
LEARNING TRUST
INSPIRED TEACHING
INSPIRING CHILDREN

Approved: Autumn 2022

Due for review: Autumn 2023

ULT Cyber Incident Response Plan

Introduction:

The Uttoxeter Learning Trust, Multi Academy Trust (MAT) IT Incident Management Plan has been developed to provide direction and focus to the handling of information security incidents that adversely affect any of the MAT schools. This plan applies to any person or entity charged by the MAT Incident Response Commander with a response to information security related incidents at the MAT.

The purpose of this document is to allow ULT MAT schools to respond quickly and appropriately to information security incidents.

Event Definition

Any observable occurrence in system, network, environment, process, workflow or personnel. Events may not be negative in nature.

Adverse Events Definition

Events with a negative consequence, this plan only applies to adverse events that are computer security related, and not those caused by natural disaster, power failures etc.

Incident Definition

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that jeopardizes the confidentiality, integrity, or availability of information resources or operations. A security incident may have one or more of the following characteristics:

- Violation of an explicit or implied security policy
- Attempts to gain unauthorized access to an Information Resource
- Denial of service to an Information Resource
- Unauthorized use of Information Resources
- Unauthorized modification of information
- Loss of Confidential or Protected information

Roles & Responsibilities:

Name	Title	Role	Contact Information	Escalation (1-3)*
Sarah Clark	Dr	Incident Response Leader		1
Andy Storer	Mr	Deputy Incident Response Leader		1
Jim McKenna	Mr	Technical Lead		1
Information Governance Unit, Corporate Services, SCC		Information Governance Officer (IGO)	Clare.nicholas@staffordshire.gov.uk 01785 278325	3
Headteacher of ULT School Affected by Cyber Incident		Local Incident Advisor	Contact details on website	3
School Technician		On Site Technician	Contact details via website	3

IT Tech Team		Support and assist Technical staff	Contact via Technical lead and help desk	4
Press & PR		Mary Hampshire PR Lore Creative	Contact the CEO	1
Sophos Rapid Response Team		Outsourced Forensic & Security Experts	01235 635329	1&2

ULT Sophos Account Details
Name: Uttoxeter Learning Trust
Sophos Central Account ID: 5708ce25-1043-743a-8ac4-ff5f0452018d

*Escalation level determines order in which notification should occur:
Notify first, required on all incidents (1, 2, 3)
Required on all moderate or high-severity incidents
Involve as needed (3)

Cyber Security Incident H*andling* Team (IHT)

- Consists of MAT Executive Leadership, IT Leadership, Data Protection Officer, and key external support providers.
- Advise on incident response activities relevant to their area of expertise.
- Maintain a general understanding of the Plan and policies of the organization.
- Ensure incident response activities are in accordance with legal, contractual, andregulatory requirements.
- Participate in tests of the incident response plan and procedures.

Responsible for internal and external communications pertaining to cyber security incidents.

Cyber Security Incident Response Team (CSIRT)

The CSIRT is comprised of ULT, IT Lead & School management and co-opted experienced personnel. The role of the CSIRT is to promptly handle an incident so that containment, investigation and recovery can occur quickly. Where third-party services are leveraged, ensure they are engaged as necessary. Roles within the CSIRT include:

IT Service Lead & Chief Executive Officer (CEO)

The CEO & ULT Tech Support Manager, or in their absence a nominated individual by the IHT takes the role of the incident response managers – and oversees and prioritises actions during the detection, analysis, and containment of an incident. They are also responsible for conveying the special requirements of high severity incidents to the rest of the organization as well as communicating potential impact to the Trustees of the MAT. Additionally, they are responsible for understanding the SLAs in place with third parties, and the role third parties may play in specific response scenarios.

- Coordinate response activities within the MAT and external resources as needed to minimize damages to information resources.
- Provide updates on response activities to MAT & School Executive Team

- Ensure service level agreements with service providers clearly define expectations of the organization and the service provider in relation to incident response.
- Review the Cyber Security Incident Response Plan (“the Plan”) to ensure that it meets policy objectives and accurately reflects the goals of the MAC. Seek Plan approval from IHT.
- Approve close of moderate or critical-severity incidents.
- Ensure lessons learned are applied/weighed based on risk for Severity 1 incidents.

Further responsibilities:

- Act as a liaison for all communications to and from the Information Governance Officer (IGO).
- Assemble a Cyber Security Incident Response Team (CSIRT).
- Ensure personnel tasked with incident response responsibilities are trained and knowledgeable on how to respond to incidents.
- Update Plan and procedures as needed based on results from testing, incident response lessons learned, industry developments and best practice.
- Review the Plan and procedures at least annually.
- Initiate tests of the Plan and procedures at least annually.
- Ensure team activities comply with legal and industry requirements for incident response procedures.
- Act as the primary Incident Response Manager, responsible for declaring a cyber security incident, managing team response activities, and approving close of Severity2 & 3 incidents.

Incident Response Team Members

The Incident Response Manager is supported by a team of technical staff that work directly with the affected information systems to research the time, location, and details of an incident. Team members are typically comprised of subject matter experts (SMEs), senior level IT staff, third parties outsourced security or forensic partners. (Sophos Rapid Response Team)

Further responsibilities:

- Assist in incident response as requested. CSIRT responsibilities should take priority over normal duties.
- Understand incident response plan and procedures to appropriately respond to anincident.
- Continue to develop skills for incident response management.
- Ensure tools are properly configured and managed to alert on securityincidents/events.
- Analyse network traffic for signs of denial of service, distributed denial of service, orother external attacks.
- Review log files of critical systems for unusual activity.
- Monitor business applications and services for signs of attack.
- Collect pertinent information regarding incidents at the request of the IRCommander.
- Consult with qualified information security staff for advice when needed.
- Ensure evidence gathering, chain of custody and preservation is appropriate.
- Participate in tests of the incident response plan and procedures.
- Be knowledgeable of service level agreements with service providers in relation to incident response.

Incident Response Framework:

The Multi Academy Trust recognises that, despite reasonable and competent efforts to protect **Information Resources**, a breach or other loss of information is possible. The MAT must make reasonable efforts and act competently to respond to a potential incident in a way that reduces the loss of information and potential harm to staff, students, parents, customers, partners, and the organisation itself.

The incident response framework is comprised of six phases that ensure a consistent and systematic approach.

Phase I – Preparation

It is essential to establish a **C**yber **S**ecurity **I**ncident **R**esponse **T**eam (CSIRT), to define appropriate lines of communication, articulate services necessary to support response activities, and procure the necessary tools.

The members of the **CSIRT** should meet regularly throughout the year, a schedule of once per term should be maintained. During the meeting, the **CSIRT** should be presented with an overview of the MATs currently risk analysis and any works required or have taken place that may affect (negatively or positively) the readiness of the MAT systems.

Incident Type	**Reporting Method**	**Available To**
Website defacement, datamodification or exposure	ULT IT Status Page Social Media Text message and Email alerts Paper comms	Internal and external (to be decided by CSIRT)
Impact on ULT IT Support functionality	ULT IT Status Page Social Media Text message and Email alerts Paper comms	Internal and external (to be decided by CSIRT)
Impact on T&L	ULT IT Status Page Social Media Text message and Email alerts Paper comms	Internal and external (to be decided by CSIRT)
Impact on business continuity	ULT IT Status Page Social Media Text message and Email alerts Paper comms	Internal and external (to be decided by CSIRT)

Phase II – Identification and Assessment

Identifying an event and conducting an assessment should be performed to confirm the existence of an incident. The assessment should include determining the scope, impact, andextent of the damage caused by the incident. In the event of possible legal action, digital evidence will be preserved, and forensic analysis may be conducted consistent with legislative and legal requirements.

Events versus Incidents

Events are observed changes in normal behaviour of the system, environment, process, workflow or personnel. Incidents are events that indicate a possible compromise of security or non-compliance with policy that negatively impacts (or may negatively impact)the organization.

To facilitate the task of identification of an incident, the following is a list of typicalsymptoms of security incidents, which may include any or all the following:

- email or phone notification from an intrusion detection tool;
- suspicious entries in system or network accounting, or logs;
- discrepancies between logs;
- repetitive unsuccessful logon attempts within a short time interval;
- unexplained new user accounts;
- unexplained new files or unfamiliar file names;
- unexplained modifications to file lengths and/or dates, especially in system files;
- unexplained attempts to write to system files or changes in system files;
- unexplained modification or deletion of data;
- denial/disruption of service or inability of one or more users to login to an account;
- system crashes;
- poor system performance of dedicated servers;
- operation of a program or sniffer device used to capture network traffic;
- unusual time of usage (e.g. users login during unusual times);
- unusual system resource consumption (High CPU usage);
- last logon (or usage) for a user account does not correspond to the actual last timethe user used the account;
- unusual usage patterns (e.g. a user account associated with a user in finance isbeing used to login to an HR database);
- unauthorized changes to user permission or access.

NOTE**: Compromised systems should be disconnected from the network rather than powered off. Powering off a compromised system could lead to loss of data, information or evidence required for a forensic investigation later.* ***Only power off the system if it cannot be disconnected from the wired and wireless networks completely.

Reporting an Event or Incident

On the discovery of a potential event – the discover of the issue (or the IT Support team member who has actioned a query which has identified an event) must immediately make the ULT IT Service Lead aware of the discovered incident. The Information Governance Officer (IGO) should also consider if a the incident should be reported to Information Commissioners Office (ico.)

Incident Scope

Determining the scope will help the IT Service Lead understand the potential business impact of the incident. The following are some of the factors to consider when determining the scope:

- How many systems are affected by this incident?
- Is Confidential or Protected information involved?
- what is/was the entry point for the incident (e.g. Internet, network, physical)?
- What is the potential damage caused by the incident?
- What is the estimated time to recover from the incident?
- What resources are required to manage the situation?
- How could the assessment be performed most effectively?

Incident Impact

Once the categorisation and scope of an incident has been determined, the potential impact of the incident must be agreed upon. The severity of the incident will dictate thecourse of action to be taken to provide a resolution; however, in all instances an incident report must be completed and reviewed by the Incident Response Commander.

Functional and informational impacts are defined with initial response activity below:

Functional Impact	Definition	CSIRT Response
None	No effect to the organization's ability to provide all services to all users.	Create ticket and assign forremediation.
Limited	Minimal effect; the organization can still provide allcritical services to all users but has lost efficiency.	Create ticket and assign forremediation, notify the IGO and IHT.
Moderate	The organization has lost the ability to provide acritical service to a subset of system users.	Initiate full CSIRT, involve the IGO and IHT
Critical	The organization is no longer able to provide somecritical services to any user.	Initiate full CSIRT, IGO, and IHT. Consider activationof the Disaster Recovery Plan

Once a potential incident has been identified, part or all of the CSIRT will be activated by the IT Service Lead to investigate the situation. The assessment will determine the category, scope, and potential impact of the incident. The CSIRT should work quickly to analyse and validate each incident, following the process outlined below, and documenting each step taken.

Informational Impact	Definition	CSIRT Response
None	No information was accessed, exfiltrated, changed, deleted, orotherwise compromised.	No action required
Limited	Public or non-sensitive data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the data owners to determine the appropriate courseof action.
Moderate	Internal Information was accessed, exfiltrated, changed, deleted, orotherwise compromised.	Notify the IGO and IHT. IGO will work with management, legal,and data owners to determine appropriate course of action.
Critical	Protected Data was accessed, exfiltrated, changed, deleted, orotherwise compromised.	Notify the IGO and IHT. IGO will work with legal to determine whether reportable, and the appropriate notification requirements.

The Incident Handling Log & Assessment Tool and Response Level table below willhelp determine the severity of the incident and urgency of response activities.

Response Level Classification		Informational Impact			
		None	**Limited**	**Moderate**	**Critical**
Functional Impact	**None**	N/A	P. 3	P. 2	P. 1
	Limited	P. 3	P. 3	P. 2	P. 1
	Moderate	P. 2	P. 2	P. 2	P. 1
	Critical	P. 1	P. 1	P. 1	P. 1

Phase III – Containment and Intelligence

Containment of the incident is necessary to minimize and isolate the damage caused. Steps must be taken to ensure that the scope of the incident does not spread to include other systems and Information Resources. Root cause analysis is required prior to moving beyond the Containment phase and may require expertise from outside parties.

Containment Strategies

Use the list of strategies below to choose the procedure(s) most appropriate for thesituation.

- stolen credentials – disable account credentials, reset all active connections, review user activity, reverse changes, increase alerting, harden from future attacks;
- ransomware – isolate the impacted system, validate the ransomware claim, contact insurance carrier, identify whether additional systems have been impacted and isolate as needed;
- if DOS/DDOS - control WAN/ISP;
- virus outbreak – contain LAN/system;
- data loss – review user activity, implement data breach response procedures;
- website defacement – repair site, harden from future attacks;
- compromised API – review changes made, repair API, harden from future attacks.

Common Containment Steps

Containment requires critical decision-making related to the nature of the incident. The IT Service Lead and other members of Executive Management should review all the containment steps listed below to formulate a strategy to contain and limit damages resulting from the incident.

All attempts to contain the threat must consider every effort to minimise the impact to the business operations. Third-party resources or interested parties may need to be notified. Where law enforcement may become involved, efforts must be made to preserve the integrity of relevant forensic or log data and maintain a clear chain-of-custody. Where evidence cannot be properly maintained due to containment efforts, the introduced discrepancy must be documented.

When evaluating containment steps, consider the following:

- Enable disposable Administrative accounts for use during the investigation and reset associated passwords if believed to have been at risk of compromise while in being used.
- Will the ability to provide critical services be impacted? How? For how long?
- Is a legal investigation or other action likely? Does evidence need to be preserved?
- How likely is the containment step to succeed? What is the result, full containment or partial?
- What resources are required to support the containment activity?
- What is the potential damage to equipment and other resources?
- What is the expected duration of the solution? (temporary, short-term, long-term, or permanent)
- Should IR team members act discretely to attempt to hide their activities from the attacker?
- Is the assistance of a third party required? What is the expected response time?
- Do interested parties (parents, staff, students, Lourdes IT clients) need to be notified? If so, when?
- Does the impact to equipment, network, or facilities necessitate the activation of the Disaster Recovery Plan?

Engage Resources

The CSIRT should select the option based on the severity of the incident, the damage incurred by and legal considerations.

	In-house investigation	Law enforcement	Private forensic specialist
Time Response	Quick response	Varies by area and agency	Quick response
Competency	Skills vary	Depends on locallaw enforcement	Highly skilled, often with law enforcement background
Preservation ofevidence	Does not ensure evidence integrity	Preserve evidence integrity and present evidence in court	Preserve evidence integrity and present evidence in court
Reputation impact	Minimal effect	Potential loss of reputation if certain incidents reach public	Potential loss of reputation if certain incidents reach public

Reduce Impact

Depending on the type of incident, the team must act quickly to reduce the impact to affected systems and/or reduce the reach of the attacker. Actions may include, but are not limited to the following:

- stop the attacker using access controls (disabling accounts, resetting active connections, changing passwords, implementing router ACLs or firewall rules, etc.);
- isolate compromised systems from the network;
- avoid changing volatile state data or system state data early on;
- identify critical external systems that must remain operational (e.g. email, clientapplication, DNS) and deny all other activity;
- maintain a low profile, if possible, to avoid alerting an attacker that you are aware oftheir presence or giving them an opportunity to learn the CSIRT's tactics, techniques,or procedures;
- to the extent possible, consider preservation of system state for furtherinvestigation or use as evidence.

Collect Data and Increase Activity Logging

Increase monitoring and packet capture on affected systems while the CSIRT investigates the scope and impact of the incident. Continue increased logging and monitoring as you move onto the Eradication and Recovery phases.

- enable full packet capture;
- collect and review system, network, and other relevant logs;
- create a memory image of impacted systems;
- take a forensic image of affected systems;
- monitor possible attacker communication channels.

Conduct Research

Performing an Internet search, consulting third party resources, and/or consulting IT using the apparent symptoms and other information related to the incident you are experiencing may lead to more information on the attack.

Notify Interested Parties

Once an incident has been identified, determine if there are others who need to be notified,both internal (Directors, School Leadership etc) and external (e.g. service providers, government, public affairs, media relations, parents and students, staff, general public,
etc.). Always follow the “need to know” principle in all communications. Most importantly,
remain factual and avoid speculation.

Depending on the degree of sensitivity of the incident, it may be necessary for Legal/Management to require employees to sign NDAs or issue gag orders to employeeswho need to be involved.

Investigation

As the CSIRT works to contain, eradicate, and recover from the incident, the investigation will be ongoing. As the investigation proceeds, you may find that the incident is not fully contained, eradicated, or recovered. If that is the situation, additional it may be necessary to revisit earlier phases (see Figure 1:PICERL Framework Model). The Containment, Eradication, and Recovery phases are frequently cyclical.

Phase IV – Eradication

Eradication requires removal or addressing of all components and symptoms of the incident. Further, validation must be performed to ensure the incident does not reoccur.
Steps to eradicate components of the incident may include:

- disable breached user accounts;
- reset any active sessions for breached accounts;
- identify and mitigate vulnerabilities leveraged by the attacker;
- close unnecessary open ports;
- increase authentication security measures (implement MFA, add geolocationrestrictions);
- increase security logging, alerting, and monitoring;
- clean installation of affected operating systems and applications.

All re-installed operating systems and applications must be installed according tosystem build standards, including but not limited to:

- applying all the latest security patches;
- disabling all unnecessary services;
- installing anti-virus software;
- applying hardened system configuration baselines;
- changing all account passwords (including domain, user and service accounts).

NOTE: It may be possible to restore the system without the need to perform a full cleaninstallation. IT personnel, at the direction of the CSIRT, will make this determination.

Phase V – Recovery

Recovery involves the steps required to restore data and systems to a healthy working state allowing business operations to be returned.

Prior to restoring systems to normal operation, it is critical that the CSIRT validate the system(s) to determine that eradication was successful, and the network is secure. Once the organization has been attacked successfully, the same attackers will often attack again using the same tools and techniques leveraged in the initial attack. Having gained access tothe compromised system(s) or network once, the attacker has more information at their disposal to leverage in future attacks.

If feasible, the system should be installed in a test environment to determine functionality prior to reintroduction into a production environment.

Furthermore, network monitoring should be implemented for as long as necessary to detectany unauthorized access attempts.

Recovery steps may include:

- restoring systems from a clean backup;
- replacing corrupted data from a clean backup;
- restoring network connections and access rules;
- communicating with interested parties about changes related to increased security;
- increasing network and system monitoring activities (short or long-term);
- increasing internal communication/reporting related to monitoring;
- engaging a third party for support in detecting or preventing future attacks.

Phase VI – Lessons Learned

The Lessons Learned phase includes post-incident analysis on the system(s) that were impacted by the incident and other potentially vulnerable systems. Lessons learned fromthe incident are communicated to executive management and action plans developed toimprove future incident management practices and reduce risk exposure.