SOUTH YORKSHIRE
PENSIONS AUTHORITY

Cyber Security Incident Management Policy

Contents

This document and its detailed policies are owned by the Corporate ICT and Digital Manager and approved by the Director as the Senior Information Risk Owner.

The Corporate ICT and Digital Manager is responsible for reviewing the content and effectiveness of this policy on a regular basis.

1 Revision History

Revision Description	Version	Revision Date	Approved date
Initial Draft	1	February 2020	
SMT Updated Draft for Board	2	July 2020	

2 Aim

2.1. The primary aim of this policy is to ensure cyber security incidents relating to the Authority's information, assets and Information Communications Technology (ICT) are managed effectively.

2.2. A copy of this document will be made available to all members of staff via SharePoint.

2.3. A master copy will be held within the ICT Section of SYPA.

3 Roles and Responsibiltiies

3.1. This policy identifies the following roles and responsibilities which may form part of the Cyber Security Incident Response Team (CSIRT).

Incident Response Coordinator

The Incident Response Coordinator is the individual who is responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation.

Primary Incident Response Coordinator	
Name :	Andy Ramsbottom
Email :	aramsbottom@sypa.org.uk
Work Telephone :	01226 772956
Mobile Telephone :	To be added internally

Alternative Incident Response Coordinator	
Name :	Julie Sykes
Email :	jsykes@sypa.org.uk
Work Telephone :	01226 772827
Mobile Telephone :	To be added internally

Incident Response Handlers

Incident Response Handlers are officers, or where necessary, outside contractors who gather, preserve and analyse evidence so that an incident can be brought to a conclusion. The incident response handlers will mainly consist of a core team of IT technicians that make up the Cyber Security Incident Response Team (CSIRT).

CSIRT Incident Response Handler	
Name :	Steve Clegg
Email :	sclegg@sypa.org.uk
Work Telephone :	01226 772831
Mobile Telephone :	To be added internally
Specialism	Networks/firewall

CSIRT Incident Response Handler	
Name :	Ben Whittaker
Email :	bwhittaker@sypa.org.uk
Work Telephone :	01226 772832
Mobile Telephone :	To be added internally
Specialism	Desktops/Clients

CSIRT Incident Response Handler	
Name :	Chris Allan
Email :	callan@sypa.org.uk
Work Telephone :	01226 772903
Mobile Telephone :	To be added internally
Specialism	Web Applications

CSIRT Incident Response Handler	
Name :	Mark Richardson
Email :	mrichardson@sypa.org.uk
Work Telephone :	01226 772185
Mobile Telephone :	To be added internally
Specialism	Web

CSIRT Incident Response Handler	
Name :	Andy Kenyon
Email :	Akenyon@sypa.org.uk
Work Telephone :	01226 772826
Mobile Telephone :	To be added internally
Specialism	Pensions Systems

CSIRT Incident Response Handler	
Name :	Terry Kirk
Email :	tkirk@sypa.org.uk
Work Telephone :	01226 772929
Mobile Telephone :	To be added internally
Specialism	Helpdesk/Patching

Data Protection Officer

Cyber security incidents involving Personally Identifiable Information (PII) or Protected Health Information (PHI) should be reported to the Authority's Data Protection Officer

Data Protection Officer	
Name :	Rob Winter
Email :	robwinter@barnsley.gov.uk
Work Telephone :	01226 773241
Mobile Telephone :	07786 525319

Legal Advice

The guidance of the Authority's Monitoring Officer should be sought if there is reason to believe that an incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit, or if there may be a need for a memorandum of understanding (MOU) or other binding agreements involving liability limitations for information sharing.

Authority Monitoring Officer	
Name :	Garry Kirk
Email :	GaryKirk@Barnsley.gov.uk
Work Telephone :	01226 773023
Mobile Telephone :	

Alternative Officer	
Name :	Martin McCarthy
Email :	MMcCarthy@syjs.gov.uk
Work Telephone :	<Insert Work Telephone >
Mobile Telephone :	

Human Resources

If an employee is suspected of causing an incident, the human resources department may be involved—for example, in assisting with disciplinary proceedings. The Authority's Human Resources department should designate one individual to handle cyber security incidents.

Primary Human Resources Representative	
Name :	Stephanie Barker
Email :	sbarker@sypa.org.uk
Work Telephone :	01226 772591
Mobile Telephone :	<Insert Mobile Telephone >

Alternative Human Resources Representative	
Name :	Lisa Darrell
Email :	ldarrell@sypa.org.uk
Work Telephone :	01226 772814
Mobile Telephone :	<Insert Mobile Telephone >

Media Handlers

Where a cyber-security incident warrants attention from the media or where the Authority wishes to release a press briefing or statement relating to a cyber-security incident or where information pertaining to a cyber-security incident must be relayed to affected individuals there will be one individual who will handle all contact and matters relating to the media, and affected individuals.

Primary Media Handler	
Name :	George Graham
Email :	GGraham@sypa.org.uk
Work Telephone :	01226 772887
Mobile Telephone :	<Insert Mobile Telephone >

Alternative Media Handler	
Name :	Relevant SMT member
Email :	
Work Telephone :	<Insert Work Telephone >
Mobile Telephone :	<Insert Mobile Telephone >

Facilities Management

Some cyber security incidents occur through breaches of physical security or involve coordinated logical *and* physical attacks. The cyber security incident response team also may need access to facilities during incident handling—for example, to acquire a compromised workstation from a locked office. Facilities management should designate one officer to handle cyber security incidents.

Primary Facilities Management Contact	
Name :	Emma Wragg
Email :	emmawragg@barnsley.gov.uk
Work Telephone :	
Mobile Telephone :	07788403978

Alternative Facilities Management Contact	
Name :	TBC
Email :	<Insert Email>
Work Telephone :	<Insert Work Telephone >
Mobile Telephone :	<Insert Mobile Telephone >

Management

Ultimately, management is held responsible for coordinating incident response among various stakeholders, minimising damage, and reporting to stakeholders, and other parties. Management endorses incident response policy, planning, budget, and staffing. The Authority's Senior Information Risk Officer (SIRO) sits at board level and provides the pivotal link between cyber security incident handling, and stakeholders. The SIRO ensures adequate resources are available as and when required to successfully handle a cyber-security incident.

SIRO	
Name :	George Graham
Email :	ggraham@sypa.org.uk
Work Telephone :	01226 772887
Mobile Telephone :	<Insert Mobile Telephone >

Head of Pensions Admin	
Name :	Jason Bailey
Email :	jbailey@sypa.org.uk
Work Telephone :	01226 772954
Mobile Telephone :	<Insert Mobile Telephone >

Head of Finance & Corporate Services	
Name :	Gillian Taberner
Email :	gtaberner@sypa.org.uk
Work Telephone :	01226 772850
Mobile Telephone :	<Insert Mobile Telephone >

Audit

The Incident Response Coordinator may require the assistance of the BMBC Internal Audit Department or where necessary, report fraudulent or criminal activity to Audit as part of the cyber security incident handling response. Audit have a key role in ensuring post incident recommendations are implemented. The Audit department should designate one officer to deal with cyber security incidents.

Primary Audit Contact	
Name :	Sharon Bradley
Email :	SharonBradley@barnsley.gov.uk
Work Telephone :	
Mobile Telephone :	07795 305846

Alternative Audit Contact	
Name :	TBC
Email :	<Insert Email>
Work Telephone :	<Insert Work Telephone >
Mobile Telephone :	<Insert Mobile Telephone >

Cyber Security Incident Response Partner

The Incident Response Coordinator may require the assistance of the 3rd party Cyber Security Incident Response Partner – ECSC Group.

Incident Response Invocation (24/7/365)	
Telephone :	0844 3763 999
Email :	incident@ecsc.co.uk
Note :	Telephone recommended method of contact

Some areas that ECSC can assist with are as follows:

- Provide regular update briefings to the Senior Management Team
- Direct internal and external response team actions
- Liaise with external agencies, such as the ICO and law enforcement
- Design external customer/client communication
- Co-ordinate with your internal or external legal advisers
- Interview staff
- Instigate actions with third-party service providers and system vendors
- Forensic investigations
- Active network traffic and log analysis

4 Incident Response Phase 1 - Detection

4.1. A cyber security incident is defined as any event that results in the compromise, misuse, or loss or Authority information, ICT services or assets.

4.2. Detection is the discovery of the event with security tools or notification from an inside or outside party about a suspected incident.

4.3. Intelligence about an event or events that may constitute an incident will originate from many sources including:

- ICT Service Desk Call
- Network Maintenance Monitoring Tools
- Partner Organisations (SYP, ISP etc.)
- Warning Advisory Services (CiSP etc.)
- Customers (Scheme members/employers)
- Other channels

4.4. All notable events will be reported to the Incident Coordinator. The Incident Coordinator will analyse the event(s) and where necessary pull together members of the Cyber Security Incident Response Team (CSIRT) to assist in the analysis. The Incident Coordinator (and CSIRT) will raise the event(s) as an incident where there is a violation or imminent threat of violation of information security policies, acceptable use policies, or other standard security practices.

4.5. Types of events that will trigger an elevation to incident status include:

- Evidence of Distributed Denial of Service
- Evidence of Malware infection such as Ransomware.
- Targeted Phishing Attack or notification that a user has opened a phishing email and clicked on any links or opened any attachments.
- Unauthorised access to Authority assets (both internally and externally).
- Unauthorised removal of data from the Authority Assets (both internally and externally).
- Evidence of successful Brute Force attacks to the network (both internally and externally).
- Unusual traffic or attempts for unusual traffic to cross the network boundary.
- Evidence of fraudulent activity.
- Evidence of privilege escalation.
- Evidence of Unauthorised alteration or tampering of any computer, server, network device or any other hardware device.
- Loss/theft of computing equipment such as a laptop.
- Unauthorised changes to data.
- Any other notable events.

5 Incident Response Phase 2 - Containment

5.1. Containment is the triage phase where the affected host(s) or system(s) is identified, isolated or otherwise mitigated, and when affected parties are notified and investigative status established. This phase may include procedures for seizure and evidence handling, escalation, and communication.

5.2. Once the Incident Coordinator (IC) (and CSIRT) have invoked an incident the IC and CSIRT will identify the affected hosts(s) and systems. The Incident Coordinator and CSIRT will establish a triage process to correctly prioritise the actions required to manage the incident and avoid rash decisions that may exacerbate the situation or lead to evidence loss.

5.3. Where necessary hosts will be isolated from the network (for example where a host has malware) or controls put in place to mitigate the incident (for example disabling a user account where there is evidence of unauthorised removal of data).

5.4. As part of the triage process the Incident Coordinator and CSIRT will decide if the incident should be escalated. This could be for many reasons for this but may include; requiring outside assistance to help manage a DDoS attack (distributed denial of service); invoking ancillary members of the cyber Security Incident Handing Plan to perform their roles; involving law enforcement agencies, etc.

5.5. The Incident Coordinator will communicate the incident details with all interested parties such as the SIRO, Information Asset Owners and relevant third parties.

5.6. The Incident Coordinator and CSIRT will determine if there is a requirement for seizure of equipment, data, logs, etc. especially where there is evidence of criminal or fraudulent activity. If there is a requirement for evidence to be handled forensically then this may be handed to external professional services to manage this aspect of the incident.

6 Incident Response Phase 3 – Investigation & Classification

6.1. Investigation is the phase where the Incident Coordinator and CSIRT determine the priority, scope, and root cause of the incident. Not all incidents will require an in depth investigation to establish the facts and determine what went wrong.

6.2. The Incident Coordinator and CSIRT will determine the cause of the incident, the effects of the incident on the Authority's assets and the scope of the incident. The incident will classified using the following scoring matrix:

Functional Impact Categories		
Category	**Definition**	**Score**
None	No effect to the organisation's ability to provide all services to all users	0
Low	Minimal effect; the organisation can still provide all critical services to all users but has lost efficiency	1
Medium	Organisation has lost the ability to provide a critical service to a subset of system users	2
High	Organisation is no longer able to provide some critical services to any users	3

Information Impact Categories		
Category	**Definition**	**Score**
None	No information was exfiltrated, changed, deleted, or otherwise compromised	0
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated	1
Integrity Loss	Sensitive or proprietary information was changed or deleted	2
Privacy Breach	Sensitive personally identifiable information (PII) of scheme members, employees, customers, etc. was accessed or exfiltrated	3

Recoverability Effort Categories		
Category	**Definition**	**Score**
Regular	Time to recovery is predictable with existing resources	1
Supplemented	Time to recovery is predictable with additional resources	2
Extended	Time to recovery is unpredictable; additional resources and outside help are needed	3
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation	4

And complete this matrix for the incident:

Cyber Security Incident Scoring	
Category	**Score**
Functional Impact	
Information Impact	
Recoverability Effort	
Total Incident Score	

6.3. An example of a Cyber Security Incident score would be as follows:

The Authority suffers a Phishing attack where a user has opened an attachment with a Ransomware payload. The Ransomware has started to encrypt files on the network.

Cyber Security Incident Scoring Category	**Score**
Functional Impact (Organisation is no longer able to provide some critical services to any users – Ransomware would require the network or parts of the network to be shutdown)	3
Information Impact (Integrity Loss – Sensitive or proprietary information was changed or deleted – Ransomware would encrypt data files)	2
Recoverability Effort (Extended -Time to recovery is unpredictable; additional resources and outside help are needed – The CSIRT would need to disinfect the network, this may require assistance from our AV supplier or other qualified partners, and once disinfected recover files from backup and ensure network defences are equipped to deal with the malware.	3
Total Incident Score	**8**

6.4. It is difficult to provide a definitive list of incidents by score as each case varies depending on the circumstances, including containment and recovery, which may reduce or escalate the level at any given point. An initial incident score will be awarded upon incident notification and may change once the facts and impact of risks has been determined.

6.5. When an incident is analysed and prioritised, the CSIRT needs to notify the appropriate individuals so that all who need to be involved will play their roles. Parties that are typically notified include:

- SIRO
- External incident response teams (if appropriate)
- System owner
- Human resources (for cases involving employees)
- Communications (for incidents that may generate publicity)
- Legal department (for incidents with potential legal ramifications)
- Law enforcement (if appropriate)

6.6. Generally the less serious incidents will involve encrypted data or low level data including near misses whereby the severity is reduced due to fortunate events. The more serious incidents will involve high level data which poses actual or potential high risk to people's rights and freedoms or to the organisation e.g. through the loss or release of highly sensitive personal or confidential business information.

6.7. Evidence will need to be gathered at various points during the investigation, but all evidence will be governed by two main rules, which are:

- Admissibility of evidence – whether or not the evidence can be used in court
- Weight of evidence – the quality and completeness of evidence

6.8. The Authority will also need to comply with relevant laws, such as the:

- Police and Criminal evidence Act 1984 (PACE)
- Data Protection Act 2018
- Computer Misuse Act 1990
- Regulation of Investigatory Powers 2000 (RIPA).

7 Incident Response Phase 4 - Remediation

7.1. Remediation is the post-incident repair of affected systems, communication and instruction to affected parties, and analysis that confirms the threat has been contained. The determination of whether there are regulatory requirements for reporting the incident (and to which outside parties) will be made at this stage. Apart from any formal reports, the post-mortem will be completed at this stage as it may impact the remediation and interpretation of the incident.

7.2. The Incident Coordinator and CSIRT will ensure any fixes required by the incident are implemented this could be applying patches, updating software, changing firewall rules, altering permissions, closing ports, recovering data, etc. The Incident Coordinator will ensure that there is a schedule of works with appropriate timescales commensurate to the disruption caused, the risk to the Authority's assets and the need to bring services back on line.

7.3. Where fixes are not immediately available, for example vulnerabilities in third party software caused an incident and the third party cannot update their software immediately (or ever) then suitable compensating controls will be designed and implemented to mitigate any future risk.

7.4. The Incident Coordinator will ensure that the fixes have been implemented and that any threat caused by the Incident has been eliminated or reduced to an acceptable Risk level.

7.5. The Incident Coordinator will record all incidents as set out in Section (9) and, where there was an actual loss of data or service, generate a formal report on the Incident for all interested parties. This report will contain all salient data such as:

- Type, scope and effect of the incident.
- Any data that was lost or altered
- Number of users effected and whether customers were effected.
- Number of services/systems taken off line and duration of interruption.
- The remediation work undertaken to fix any issues including the work of any third party.
- Validation that the remediation work has eliminated or mitigated the Risk.
- Members of the Cyber Security Incident Handling Plan that were invoked, their scope in relation to the incident and their performance.
- Any interaction with law enforcement agencies including evidence seized.
- The external bodies that were contacted to report the incident.
- An estimate of the cost of the incident including any identifiable actual costs such as overtime, purchase of equipment/software, purchase of external services and an estimate of things such as the cost of loss of service (staff being paid but unable to work without computer systems, projects delayed due to lack of online services, lack of customer processing, etc.), reputational damage, etc.

7.6. The Incident Coordinator (and DPO where relevant) will report the incident to the appropriate bodies as necessary.

8 Incident Response Phase 5 - Recovery

8.1. Recovery is the analysis of the incident for its procedural and policy implications, the gathering of metrics, and the incorporation of “lessons learned” into future response activities and training.

8.2. The Incident Coordinator, CSIRT and any members of the CSIRT that was invoked for the incident will hold a formal post incident meeting where the incident involved an actual loss of data or service

8.3. The purpose of this meeting is to assess the performance of the team in relation to how the incident was managed and whether any improvements should be introduced; examine whether the Authority should update any Security Policies or Procedures in relation to the Incident; determine if staff training should be updated or implemented in relation to the incident; consider whether additional technical controls or tools should be introduced to reduce the risk of a similar incident occurring; examine the communication elements of the incident to ensure they were handled effectively; to determine if there were any gaps in the plan; whether the correct personnel were available when required; whether other personnel or roles should be formally identified and added to the plan; etc.

9 Documentation

9.1. The Incident Coordinator is responsible for ensuring that the Incident is documented appropriately.

9.2. All documents relating to an Incident will be stored together in the Incident Response repository within its own folder and should include a Cyber Security Incident Log, copies of any evidence salient to the incident (e.g. incident alert, logs, equipment seized, etc.), emails relating to the incident, communications (press release, video, audio, copies of web statements, etc.), schedule of remediation tasks, schedule of any direct costs (overtime, software, etc.), post Incident report, reports sent to third parties, interactions with law enforcement agencies, etc.