West Mercia POLICE		POLICY
Security Classification	**OFFICIAL**	
Disclosable under Freedom of Information Act 2000	Yes	

POLICY TITLE	**Cyber Incident Response**
REFERENCE NUMBER	**WMP199**
Version	**1.0**

POLICY OWNERSHIP	
DIRECTORATE	BUSINESS SERVICES
BUSINESS AREA	DIGITAL SERVICES

INITIAL IMPLEMENTATION DATE	**November 2022**
NEXT REVIEW DATE:	**November 2025**
RISK RATING	**LOW**
EQUALITY ANALYSIS	**LOW**

West Mercia Police welcome comments and suggestions from the public and staff about the contents and implementation of this policy.
Please e-mail policiesandprocedures@westmercia.pnn.police.uk

1.0 POLICY OUTLINE

Cyber incidents can quickly escalate and become a significant business disruptor requiring both business continuity and consequence management considerations. Much of the digital response will be managed within the IT Security environment and aligned to this policy and associated plans and procedures. However, early consideration should also be given to engaging Business Continuity, Policy Area and Resilience Leads where they exist to manage wider impacts.

2.0 PURPOSE OF POLICY

The purpose of this policy is to outline the requirements to provide documented operational structures, processes, and procedures to West Mercia Police (WMP) personnel, so that they can effectively respond to cyber incidents that may impact the function and security of digital assets, information resources, and business operations.

This policy will set out requirements that will assist WMP in identifying, managing, investigating, and remediating various types of cyber incidents. It describes the processes for initiating a response and establishing the structure needed to ensure response execution.

Business Continuity, Policy Area and Resilience leads in the organisation must therefore be familiar with this policy and how its requirements are delivered through the force Cyber Incident Response Plan (CIRP).

To provide assurance of security and compliance related objectives, this policy may be shared with interested internal and external parties who are not authorised to view the force CIRP.

3.0 IMPLICATIONS of the POLICY

The effective operation of this policy and associated procedures will support the delivery of effective policing services, assist in reducing costs, system downtime, corruption of data and protect people from harm by ensuring that information is secure, accurate and available to the right people at the right time.

WMP is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees of WMP and third-party users of Force Systems, who may be accountable for any breaches of Information Security for which they may be held responsible.

This policy and associated plans and procedures support compliance with legal, national and best practice standards including, but not limited to:

- Freedom of Information Act 2000
- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Computer Misuse Act 1990
- Official Secrets Act 1989
- HMG Security Policy Framework
- Governance and Information Risk Return

- ISO27001

This document is primarily aimed at staff supporting WMP information systems. Therefore, all WMP employees, officers, staff, partner agencies and third-party users of WMP systems in applicable roles must comply with this policy and its associated procedures, and where requested, to demonstrate such compliance. Failure to comply with the policy may be regarded as a disciplinary offence and may be dealt with subject to misconduct proceedings. In serious cases, this may be treated as gross misconduct and may result in summary dismissal.

4.0 POLICY FRAMEWORK

WMP Digital Services (DS) shall maintain a documented CIRP which will align with the following industry best practices:

- NCSC Cyber Incident Response
- The Standard of Good Practice for Information Security 2018
- ISO/IEC 27035: 2016 Information Security Incident Management

The CIRP shall be stored securely, both in digital and hard copy formats and access granted on a need-to-know basis only.

The CIRP shall document the following sections in detail to allow an effective response to a cyber incident:

- The clear identification of incident management roles and responsibilities aligned to a 'Responsible, Accountable, Consulted and Informed' (RACI) matrix for each incident response task.
- A resilient communications plan for internal and external communications in the event of an incident.
- A defined Cyber Incident Response methodology, aligned to best practice.

The CIRP shall also reference up to date procedural documentation that provides operational-level details specific to handling the various incident types.

The CIRP shall be reviewed for alignment with industry best practice on an annual basis or in response to an incident review and closure session.

Any changes to the CIRP shall be subject to Head of DS approval.

The CIRP shall be tested periodically through either a table-top exercise or simulation test using industry approved tools. At least one form of each exercise should take place annually to ensure the CIRP remains fit for the current environment. A live incident which tests WMPs response to all aspects of the CIRP may replace one of these periodic tests only.

The CIRP cannot anticipate and provide guidance for all potential incidents. Management roles and incident responders shall consider the current situation, business impact, and security needs of WMP and balance those against the guidance and recommendations provided by the CIRP.

Associated Documents

- Cyber Incident Response Plan v1.0

This document is available in both online and offline formats to authorised personnel on a need-to-know basis. To request access please contact the DS Security Operations Manager or IT Security Officer.

5.0 CONSULTATION

Business Lead/ Chief Officer Consulted	***Date Consulted***
Simon Bennett/ Rachel Hartland-Lane	July 2022/ August 2022

The following have been identified as key stakeholders who will be part of the consultation exercise.

Head of Digital Services
Security Operations Manager
IT Architecture Manager
DS Operations Manager
Information Security Manager
UNISON
Critical Friends Group

6.0 DOCUMENT HISTORY

Date	**Author / Reviewer**	**Amendment(s) & Rationale**	**Date of Approval / Adoption**
July 2022	D Archer	New Policy	JNCC 08/11/2022

7.0 ASSESSMENT AND ANALYSIS

The Equality Analysis (EA), Health & Safety Assessment (HAS) and Risk Assessment (RA) associated with this document are available on request.

8.0 DATA PROTECTION IMPACT ASSESSMENT

- Is a DPIA required? – No, as agreed by Audit, Risk and Compliance on 22/07/2022

9.0 MONITORING / EVALUATION

The Monitoring and review of this policy is the responsibility of the policy owner