# CYBER STANDARDS DOCUMENT

## *NCSP Cyber Incident Management*

**ABSTRACT**:
This Standard specifies the minimum requirements regarding cyber threat and incident processes and actions. It aims to provide members of the policing community with clear direction to manage incidents associated with cyber-attacks and cyber incidents.

**APPENDIX A**: Terms and Abbreviations

| | |
|---|---|
| **ISSUED** | September 2024 |
| **PLANNED REVIEW DATE** | October 2025 |
| **DISTRIBUTION** | Community Security Policy Framework Members |

**POLICY VALIDITY STATEMENT**
This standard is due for review on the date shown above. After this date, this document may become invalid.

Cyber Standard users should ensure that they are consulting the currently valid version of the documentation.

# CONTENTS

Community Security Policy Commitment....3
Introduction....3
Owner....3
Purpose....3
Audience....4
Scope....5
Requirements....5
Communication approach....16
Review Cycle....16
Document Compliance Requirements....16
Equality Impact Assessment....16
Document Information....17
Document Location....17
Revision History....17
Approvals....17
Document References....18

## Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This standard in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing requirements regarding cyber threat and cyber incident processes and actions.

## Introduction

This standard specifies the minimum requirements regarding cyber incident processes and actions. It aims to provide policing, PDS (Police Digital Service) and third parties working for policing with clear direction to manage cyber incidents.

This standard also strives to support the National Policing Cyber Security Strategy published in June 2024 to meet its five strategic objectives:

- Manage cyber security risk
- Protect against cyber attacks
- Detect cyber security events
- Minimise the impact of cyber security incidents
- Develop the right cyber security skills knowledge and culture

## Owner

National Chief Information Security Officer (NCISO).

## Purpose

The purpose of this standard is to establish formal requirements, which detail a Security Incident Management Framework and Security Incident Management Process that should be applied within each police force and PDS.
In addition, the requirements stated in this standard are mapped across the following industry standard frameworks:

- ISO 27002:2022

- CIS Controls
- NIST Cyber Security Framework v1.1
- Information Security Forum (ISF) Statement of Good Practice (SoGP)

This standard helps members of the community of trust to comply with the National Community Security Policy (NCSP) Incident Management Policy heading to:

- Establish a comprehensive and approved information security incident management framework (including a designated incident response team; access to cyber incident investigators and forensics experts; threat-related information; and technical investigation tools), which is supported by a process for the identification, response, recovery, and post incident review of information security incidents.
- Encourage an organisation wide culture of reporting of suspect or actual security events.

## Audience

Members of the Policing Community of Trust must read and adopt this standard.

More specifically the standard is targeted at, those who are needed to respond to or are involved in the response and recovery measures of a cyber incident or cyber-attack, either on behalf of national policing or at a local force level. The following should also be aware of the content of this standard, in order that they can provide appropriate oversight and governance of threat and incident management within policing:

- Senior Information Risk Owners (SIROs)
- Information Asset Owners (IAOs)
- Information & Cyber risk practitioners and managers
- Auditors providing assurance services to PDS or policing.

Any person who accesses or processes national policing systems, information or local force systems should be aware of the requirement to report actual or suspected security incidents as described in this standard.

Finally, policing's reliance on third parties means that suppliers acting as service providers or developing products or services for PDS or policing, should also be made aware of and comply with the content of this standard, in relation to their work on policing systems and data.

## Scope

1. This standard applies wherever policing information is processed or stored, National policing IT systems, applications, or service implementations.
2. The security control requirements laid out in this standard are vendor agnostic and applicable for all IT systems, applications, or service implementations that are provisioned for policing community of trust use.
3. The requirements of this standard should form part of third-party supplier contractual obligations where Policing information is processed or stored on behalf of any member of the policing community of trust.
4. The requirements of this standard can be considered as part of any agreements with third parties who are not suppliers, who have access to Policing information.

## Requirements

This section details the minimum requirements cyber-attack response, security incident management framework and process to protect policing from the loss of confidentiality, integrity or availability of the data or loss of availability of the systems and services it relies upon to meet policing outcomes.

It is broken down into 4 sections;

1.0 Cyber attack response readiness
2.0 Security incident management framework
3.0 Security incident management process
4.0 Emergency fixes

| Reference | Minimum requirement | Control reference | Compliance Metric |
|---|---|---|---|
| **1.0 Cyber Attack response readiness** | | | |
| **1.0 Response** | Each policing community member, PDS, Partner & 3rd party Supplier should ensure that there are documented standards, processes and procedures to respond to sophisticated, targeted cyber-attacks at each stage of the cyber-attack kill chain. * These will include National Cyber standards and procedures.<br><br>These standards should consider all tactics under the MITRE ATT&CK Framework including:<br>• Reconnaissance, typically using informative security controls (e.g., threat intelligence and an insider threat programme)<br>• Initial Access Controls, typically using a combination of preventative and detective security controls such as strong multi-factor authentication, and encryption at all stages of the information lifecycle.<br>• Maintaining control, typically using security controls such as strict audit of user accounts, and scanning systems and networks for anomalies<br>• Identifying potentially compromised information, typically using security controls such as continuous monitoring and Data Loss Prevention (DLP)<br>• Exploitation of information, typically performing threat intelligence, enhanced due diligence measures, and monitoring online activity for details about stolen material. | SoGP TM1.5<br><br>ISO27001: 2022<br><br>CISv8.1 1.1-1.5, 2.1-2.4, 3.1-3.14, 4.1-4.12, 5.1-5.5, 6.1.-6.8, 7.1-7.7, 9.1-9.7, 10.1-10.7, 12.1-12.8, 13.1-13.10, 14.1-14.9<br><br>NIST ID.AM, ID.BE, ID.GV, ID.RA, ID.RM, ID.SC, PR.AC, PR.AT, PR.DS, PR.IP, PR.MA, PR.PT, RS.IM | Defined process including documented decision making.<br><br>NMC Cyber Liaison Officers can confirm if plans have been reviewed and / or tested<br><br>Documented, agreed, implemented standards, procedures and processes.<br><br>Evidence of 3rd party supply standards & procedures. |

| | | | |
|---|---|---|---|
| **1.1 Process** | To understand the risks and impact associated with cyber-attacks, there should be a thorough review of potential attacks highlighting any vulnerabilities associated with:<br><br>• people (e.g., successful social engineering attempts and potential insider threats)<br>• processes (e.g., a weakness in any one process that a threat actor could exploit as part of the attack)<br>• technologies (e.g., an unpatched operating system vulnerability or vulnerable legacy system).<br><br>To achieve this:<br>• systems, third-parties, software, and information systems should be inventoried, and risk assessed.<br>• models of governance developed including organisational cybersecurity policies.<br>• identity, credential, and authorised devices are documented.<br>• all users should be informed and trained.<br>• vulnerability management plan developed and maintained.<br>• a baseline of network operations and expected data flows for users and systems should be established and managed.<br>• the network, the physical environment and personnel activity should be monitored to detect potential cybersecurity events.<br>• ***-see Appendix A Terms and Abbreviations** | NIST<br><br>ID.AM<br>ID.GV-4<br>PR.AC<br>PR.AT-1<br>ID.RA | Documented processes and supporting records<br><br>Maintained, current physical asset inventory<br><br>Information Asset Register<br><br>Established, monitored governance<br><br>User cyber awareness programme.<br><br>Identity & Access management solution<br><br>Vulnerability management solution supported by processes & procedures.<br><br>Network inventory, monitoring & alerting. |

| 2.0 Security Incident Management Framework | | | |
|---|---|---|---|
| **2.0 People** | **People.** Each policing community member, PDS, Partner & 3rd party supplier should have an established Cyber Incident Management Framework which is made up of specialist teams (or individuals) who:<br><br>• Have defined and documented roles and responsibilities with sufficient skills or experience in managing incidents.<br>• Have the authority to make critical business decisions and escalate as required.<br>• Can communicate successfully with key stakeholders both internally and externally. | SoGP TM2.1, TM2.2, TM2.3, TM2.4<br><br>ISO27001: 2022 5.24, 5.26, 5.29<br><br>ISO27001/2 12.4.1, 16.1.1, 16.1.4, 16.1.5<br><br>CISv8.1 17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7<br><br>NIST RS.IM.1, RS.IM.2, RS.OP.1, RS.RP.1 | NMC Cyber Liaison Officers can confirm if plans have been reviewed and / or tested<br><br>Documented, approved cyber incident management framework.<br><br>Records of reviews, approvals and invocations.<br><br>Associated records including previous incidents and outcomes. |
| **2.1 Technology**. | The framework should also have documented and detailed processes/ procedures which specify:<br>• The dedicated technology tooling (SIEM) and incident analysis resources used to handle incidents quickly and effectively.<br>• Details about how Cyber Security incidents should be recorded and maintained. | | |

| | | | |
|---|---|---|---|
| **2.2 Knowledge**. | Information required to assist with the management of incidents should be documented and easily accessible to the specialised teams in place and look to include:<br><br>• Contact details for all internal and external stakeholders, agencies, and partners.<br>• Access to relevant security-related event logs, for example those produced by devices, applications, security products and systems.<br>• Access to BAU cyber incident management process and Incident Response Plan.<br>• Detail of an agreed escalation process internally within the force and externally for all Partners.<br>• Threat intelligence and the results of threat analysis<br>• Technical details of 3rd party vendors used across the estate. | NIST<br><br>ID.SC<br>PR.AT<br>PR.IP<br>RS.RP<br>RS.CO | Contact register.<br><br>Cyber incident management plan.<br><br>Inventory / record of knowledge assets – information asset register.<br><br>Established protective monitoring that meets business needs.<br><br>Third party register. |
| **2.3 Control** | Legal and regulatory requirements should be identified and met during the incident response to include:<br><br>• Security related laws and regulations relevant to the incident.<br>• Incident reporting timescales (e.g., Notifying the Information Commissioner's Office within 72 hours of a data breach being identified)<br>• Any specific compliance requirements<br>• Collection of forensic electronic evidence | NIST<br><br>ID.GV | Processes in place which take account of requirements.<br><br>Incident recording & management system.<br><br>Forensic readiness policy. |

| 3.0 Security Incident Management Process | | | |
|---|---|---|---|
| **3.0 Process** | Each policing community member, PDS, Partner and 3rd party supplier should ensure that Cyber security incidents are identified, responded to, recovered from, and followed up using an approved cyber security incident management process. | NIST<br><br>ID.SC | Cyber incident management plan & processes.<br><br>Incident recording & management system. |

| | | | |
|---|---|---|---|
| **3.1 Incident Response Plan.** | All policing community members must have a documented Cyber Incident Response Plan. This plan must describe incident response procedures including:<br><br>• Roles & Responsibilities<br>• Contacts & Escalation Process<br>• Definition & Categorisation of an Incident<br>• Training & Exercising<br>• Overview of Existing Tools & Processes used in Prevention of a Cyber Incident<br>• Incident Communication Plan<br>• Major Incident Declaration Plans<br>• Incident Reporting<br>• Incident Plan Activation<br>• Triage & Impact Assessment Process<br>• Incident Analysis Process<br>• Containment & Eradication Procedure<br>• Remediation & Recovery Process<br>• Post Incident Review Template & Process<br>• Any Links out to Relevant Documentation or Interfaces to other Processes. These must include as a minimum:<br>• A network topology of the IT estate.<br>• Playbooks (or runbooks) for the detailed incident response process for specific cyber incidents.<br>• BCP and Disaster Recovery documents.<br>• Technical Backup & Recovery plan for data, systems & devices.<br>• (General) Major Incident Plan for your organisation.<br>• Communications strategy.<br>• Priority Matrix for critical systems and assets (which must include in | ISF TM2.2, TM2.3, TM2.4<br><br>ISO27001/2 16.1.1, 16.1.2, 16.1.6<br><br>CIS v8.1 7.2, 17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8<br><br>NIST DE.AE.1, DE.AE.2, DE.AE.4, ID.GV.2, PR.IP.1, PR.IP.10, RC.CO.3, RC.IM.1, RC.RP.1, rS.AN.2, RS.AN.4, RS.CO.1, RS.CO.2, RS.CO.3, RS.CO.4, RS.CO.5, RS.IM.1, RS.IM.2, RS.MI.1, RS.MI.2, RS.MI.3, RS.RP.1 | Inventory of 3rd party suppliers. Registry of legal & regulatory requirements. Forensic readiness policy / plan.<br><br>NMC Cyber Liaison Officers can confirm if plans have been reviewed and / or tested.<br><br>Documented, approved, maintained incident response plan. |

| | | | |
|---|---|---|---|
| | what orders systems will be brought back online in the event of a full or partial outage).<br>• Safeguarding plans and the trigger plan for activating these to communicate with data subjects who may have been affected by data loss, compromise or access.<br>• The Incident Response Plan must be reviewed and updated annually as a minimum requirement or as a result of testing / invocations. | | |
| **3.2 Recording an Incident.** | All cyber security incidents should be recorded in a log or ITSM system. As a minimum they should:<br>• Be categorised and classified and given a reference.<br>• Contain a description of the incident and the impact.<br>• Contain all actions taken during the incident and any evidence gathered.<br>• Include a detailed Timeline of Events.<br>• Include a start and end date and time.<br>• Include a resolution reason. | NIST<br><br>RS.CO | Records of incidents and actions taken. |

| | | | |
|---|---|---|---|
| **3.3 Collaborative Working**. | When responding to a cyber incident, policing community members and NMC should support this with collaborative actions including:<br><br>• Sharing logs from relevant security or IT products, systems, and applications to complete analysis<br>• Sharing findings analysis and investigations<br>• NMC Incident Response will respond to and acknowledge all force queries within 30 minutes.<br>• NMC Incident Response will provide recommendations of actions to take, to policing community members, on their investigative findings. | NIST<br><br>ID.GV<br>ID.SC-5 | Records of incidents and actions taken. |
| **3.4 War Gaming / Red Teaming**. | War Gaming / Red Teaming. Regular cyber security exercises should be performed to test the strength and validity of the Incident Response Plan, decision making capabilities and aid continuous improvement. This as a minimum requirement, should be carried out annually. There should be multiple exercises built to cover different cyber incident scenarios such as:<br><br>• DDoS<br>• Malware<br>• Ransomware<br>• Phishing/ Smishing<br>• Data Breach<br><br>The Incident Response Plan must be reviewed and updated as a result of exercises. | NIST<br><br>ID.GV<br>ID.SC-5 | Records of collaborative working internally and externally. |

| | | |
|---|---|---|
| **3.5 Communications.** | As described in the National Cyber Security Incident guideline all incidents involving police data or systems that have been considered cyber related by the Information Security Officer must be reported to the NMC for visibility.<br><br>Reviews of all information related incidents should be undertaken including trending. This will help ascertain the effectiveness of security controls as well as feedback into risk assessments.<br>Communications should be:<br><br>• Tested regularly to ensure they are fit for purpose.<br>• Have a contingency plan in place to move to secondary methods if the primary methods are affected by a cyber incident.<br><br>Communication plans should include:<br><br>• The strategy for the CSIRT (Cyber Security Incident Response Team) to communicate with each other during the lifecycle of an incident.<br>• The strategy for communicating the incident to employees.<br>• The strategy for (internal) Executive Level communications.<br>• The strategy for external communications for 3rd party stakeholders.<br>• The strategy for external communications to the media and members of the public.<br>• The strategy for communications to data subjects whose data has been compromised, exfiltrated or accessed.<br>• Provisions for managing employee and user wellbeing during the cyber incident lifecycle.<br><br>Forces and organisations should encourage the internal reporting of all non-cyber events, incidents, breaches or near misses that affect policing information. Examples include physical security, failures to follow policy, theft or damage. | Records of designing and undertaking exercises.<br><br>Findings & learning outcomes.<br><br>Documented communication plans.<br>Records of testing and reviews.<br><br>Management reviews of incident reports.<br><br>Incident trending and reviews against risks and controls. |

| | | | |
|---|---|---|---|
| | • | | |
| **3.6 Post Incident Reviews.** | Following the recovery of a critical cyber incident a debrief or PIR must be completed by both PDS NMC and the affected force or system owner:<br><br>• To complete root cause analysis to identify the cause of the incident<br>• Perform any forensic investigations if required from the event.<br>• Record and track all actions raised follow up to ensure all are implemented.<br>• To review existing processes and procedures to determine their capabilities and if they were fit for purpose during the incident. Any agreed changes to processes following this should be tested and documented.<br>• Document the PIR in a report.<br>• Recommend that a bi-annual aggregate review of all PIR's in the preceding 6 to 12 months be undertaken to identify any trends or developments.<br>• Management reviews of incidents should help ascertain the effectiveness of security controls as well as feedback into risk assessments. | NIST<br>RC.RP-1<br>RC-IM-1 | Management reviews<br>Evidence of learning / tests<br><br>Records of previous incidents and outcomes.<br><br>PIR reports<br><br>Defined schedule of reviews of all incidents including trends and risk reviews. |
| **4.0 Emergency Fixes** | **Recommendations**. NMC (PDS) will provide recommendations to forces for any remediations and emergency fixes in response to a cyber incident. Forces and systems should have documented procedures for applying emergency fixes to business applications and technical infrastructure (including software and end points). | ISF TM 2.3 | NMC Cyber Liaison Officers can confirm if plans have been reviewed and / or tested |

## Communication approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Presentation to the National Cyber Policy & Standards Board (NCPSB) for approval.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

For external use (outside PDS), this standard should be distributed within IT and information security teams to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with force SIROs / Security Management Forum. Consideration should also be given to raising awareness amongst force personnel of the implementation of this standard where it may affect them.

Measurables generated by adopting this standard can also form part of regular cyber management reporting.

## Review Cycle

This standard will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the standard continues to meet the objectives and strategies of the police service.

## Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

## Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)

## Document Information

**Document Location**

National Standards Portal

**Revision History**

| Version | Author | Description | Date |
|---|---|---|---|
| 0.1 | PDS Cyber | Initial version | 20/06/23 |
| 0.2 | PDS Cyber | Updated for review | 20/06/23 |
| 0.3 | PDS Cyber | Updated for following NCPSWG comments. Inclusion of Appendix A for term | 11/09/23 |
| 1.1 | PDS Cyber | Annual review | 22/08/24 |
| 1.2 | PDS Cyber | Removed threat section and updated to align with V1.4 CSP | 13/09/24 |

**Approvals**

| Version | Name | Role | Date |
|---|---|---|---|
| 1.0 | National Cyber Policy & Standards Board | National authority for approving cyber standards | 30/11/23 |
| 1.2 | National Cyber Policy & Standards Board | National Cyber Policy & Standards Board | 26/11/24 |

**Document References**

| Document Name | Version | Date |
|---|---|---|
| ISF - Standard of Good Practice (for Information Security) | v2024 | 03/2024 |
| ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls | v2022 | 02/2022 |
| CIS Controls | v8 | 05/2021 |
| NIST Cyber Security Framework | v1.1 | 04/2018 |
| CSA Cloud Controls Matrix | v4 | 01/2021 |
| 10 Steps to Cyber Security - NCSC.GOV.UK | Web Page | 05/2021 |

**Appendix A – Terms and Abbreviations**

Based upon National Institute of Standards & Technology (NIST) and National Cyber Security Centre

| Term | Abbreviation | Brief Explanation |
|---|---|---|
| **Alert** | | A brief, usually human-readable, technical notification regarding current vulnerabilities, exploits, and other security issues. Also known as an advisory, bulletin, or vulnerability note. |
| **Anomalies** | | Condition that deviates from expectations based on requirements specifications, design documents, user documents, or standards, or from someone's perceptions or experiences. |
| **Attack** | | Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. |
| **Attacker** | | Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome. |
| **Breach** | | An incident in which data, computer systems or networks are accessed or affected in a non-authorised way. |
| **Data Breach** | | A breach leading to loss of data. |
| **Data Loss Prevention** | DLP | A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of NSS information. |
| **Distributed Denial of Service** | DDOS | When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests. Distributed uses numerous hosts to perform the attack |
| **Event** | | Any observable occurrence in a network or information system. |

| Term | Abbreviation | Brief Explanation |
|---|---|---|
| **Exploit** | | May refer to software or data that takes advantage of a vulnerability in a system to cause unintended consequences. |
| **Forensics** | | The practice of gathering, retaining, and analysing computer-related data for investigative purposes in a manner that maintains the integrity of the data. |
| **(Cyber) Incident** | | A breach of the security rules for a system or service - most commonly:<br>• Attempts to gain unauthorised access to a system and/or to data.<br>• Unauthorised use of systems for the processing or storing of data.<br>• Changes to a systems firmware, software or hardware without the system owner's consent.<br>• Malicious disruption and/or denial of service. |
| **Impact** | | The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. |
| **Intelligence** | | Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence. |
| **Kill-Chain** | | Developed by Lockheed Martin, **the Cyber Kill Chain®** framework is part of the **Intelligence Driven Defence®** model for identification and prevention of cyber intrusions activity.<br>The model identifies what the adversaries must complete in order to achieve their objective. |

| Term | Abbreviation | Brief Explanation |
|---|---|---|
| **Kill-Chain cont.** | | The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures. |
| **Malware** | | Malicious software - a term that includes viruses, trojans, worms or any code or content that could have an adverse impact on organisations or individuals. |
| **MITRE Attack** | MITRE ATT&CK | MITRE ATT&CK ® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.<br><br>Adversarial Tactics, Techniques, and Common Knowledge |
| **Phishing** | | Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website. |
| **Post Incident Review** | PIR | A Post Incident Review is a document that is created after a cybersecurity incident has occurred: it is an in-depth analysis of what happened, how it happened, and what steps can be taken to prevent similar incidents from happening in the future. |
| **Ransomware** | | Malicious software that makes data or systems unusable until the victim makes a payment. |
| **Reconnaissance** | | A process of gathering information about the target organization. For an attacker, the first step of hacking involves collecting crucial information regarding the target so the attacker can then utilize this information to exploit and penetrate the target networks. |
| **Recover** | | Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. |

| Term | Abbreviation | Brief Explanation |
|---|---|---|
| **Respond** | | Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. |
| **SIEM** | | Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. |
| **Smishing** | | Phishing via SMS: mass text messages sent to users asking for sensitive information (e.g. bank details) or encouraging them to visit a fake website. |
| **Threat** | | Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. |
| **Triage** | | Triage is an incident response technique for identifying and prioritizing your response to cyber threats. It helps you analyze threat alerts to determine the most harmful or impactful ones and prioritize them over others to prevent damage to your system. |
| **Tactics, Techniques and Procedures** | TTP | The behaviour of an actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique. |
| **Vulnerability** | | A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system. |

| Term | Abbreviation | Brief Explanation |
|---|---|---|
| **War Gaming/ Red Teaming** | | A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team. |