Information Security Policy

This document is part of North Yorkshire Police policy to which all Chief Constable personnel are required to adhere to.

Policy Statement

The purpose of this policy is to protect North Yorkshire Police (NYP) information assets from all threats, whether internal or external, deliberate or accidental. It is concerned with the preservation of:

- Confidentiality - ensuring that information is accessible only to those authorised to have access, disclosed only to those authorised to receive it, and so disclosed only for police purposes;
- Integrity - safeguarding the accuracy and completeness of information and information processing methods;
- Availability - ensuring that authorised users have access to information and associated assets when required.

All staff, regardless of being Chief Constable personnel or the functions provided by the Police, Fire and Crime Commissioner, including permanent, temporary, volunteers, contract staff, delivery partners and third party suppliers, have a responsibility for safeguarding NYP's information assets and ensuring the security of those assets in their respective hosting environment i.e. on premise or in a cloud environment. This Force Information Security Policy (FISP) document will help you to understand your responsibilities and fulfil them.

NYP's approach to information security is to balance the business requirements of the organisation with the potential harm and risk of an information security incident and the cost and logistics of implementing security controls.

Key Drivers and Outcomes

Compliance with Home Office Police Digital Services (PDS) PSNP Approval Controls

The Security Assessment for Policing (SyAP), previously the GIRR, sets prescriptive security controls for forces to achieve to maintain a baseline level of security to connect to the PSNP network, to both protect Police information and prove our place in the policing community of trust and facilitate easier sharing of information between Police forces. The SyAP controls prescribe network security controls which NYP evidence compliance with annually. The model runs parallel with the Security Policy Framework (SPF) and the Information Systems Community Security Policy (CSP).

The intended outcome of this FISP is to:

- enable NYP to use and share its information with confidence;
- have in place suitable safeguards to ensure the confidentiality, integrity and availability of NYP information systems; and
- ensure all NYP's contractual, statutory and regulatory obligations for information security are met.

The specific objective of the controls within this policy and related procedures is to enable NYP to conduct its operations, whilst reducing to an acceptable level the risk of business damage by preventing and minimising the impact of information security incidents.

The full definition of what constitutes a security incident and how to handle it, can be found in the Security Incident Reporting and the Security Incident Handling procedures.

Authority and Responsibility

The Chief Constable, acting as Force Accounting Officer, has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. This is evidenced in the Annual Governance Statement (AGS). The AGS sets out the Chief Constable and Commissioner Decision Making and Scrutiny Arrangements, a key feature of which is the Information Assurance Board. This Board has a role in assessing compliance with mandatory requirements which must explicitly cover information risk. Where appropriate areas for development will be recorded in the AGS.

The Deputy Chief Constable as the Senior Information Risk Owner (SIRO), is required to be familiar with information risks and NYP's response to risk. The SIRO owns the information risk policy and risk assessments, acts as an advocate for information risk with the Chief Officer Team and other internal discussions and is responsible for providing written advice to the Force Accounting Officer on information assurance risks and any identified areas for development captured in the AGS.

The SIRO is required to understand how NYP's business goals may be impacted by information systems' failures and information asset loss. The ownership of risk is a strategic responsibility. Although supported by the information assurance resource, including the Force Accreditor, namely the Information Security Officer, the ownership of risk remains with the SIRO.

Heads of Functions have overall responsibility for the satisfactory implementation and maintenance of the general security requirements contained in this policy. Specific responsibilities include:

- ensuring supervisors and managers within Departments are aware of NYP's security requirements as defined in this policy, other relevant NYP policies/procedures and other systems operating procedures;
- ensuring that information security is included on the agenda of relevant senior management team meetings;
- ensuring security incidents are reported to the Information Security Officer and, where necessary, investigated and escalated;
- raising specific security issues with the Information Security Officer, SIRO or Information Assurance Board (IAB), as appropriate.

Information Assurance Governance

The Force Information Assurance Board (IAB) is chaired by the SIRO and its membership comprises of Heads of Functions and nominated representatives from specialist areas. The IAB covers aspects of information assurance including:

- PSNP compliance
- Security reporting and handling
- Compliance with all legislative and regulatory requirements
- Other matters relating to information risk and the management thereof

For further information regarding the responsibilities of the IAB please refer to the IAB Terms of Reference.

Individual Roles/Functions and Responsibilities

The following roles are necessary to ensure that PSNP requirements and SPF compliance are attained, accreditation is maintained and that information assurance in general is successfully integrated within NYP.

The Information Security Officer (ISO) provides a focal point for information security and compliance issues. The ISO reports to the IAB regarding the following:

- identifying and assessing the risks to information security;
- identifying information security safeguards and countermeasures;
- maintaining a satisfactory level of security awareness-
- reporting security incidents to the IAB and to the information assurance section of the Home Office in line with the requirements of the CSP and Security Policy Framework (SPF);
- monitoring the proper operation of security controls within NYP and, also, in cases where a third party has access to information assets owned or managed by NYP;
- investigating weaknesses in security control measures and security incidents;
- providing guidance and advice on legislation, directives and guidelines relating to information security;
- ensuring the FISP portfolio is current, properly controlled and distributed;
- ensuring appropriate levels of compliance with the FISP, including the establishment of relevant security operating procedures (SyOPs);
- monitoring NYP general information security controls;
- acting as the main point of contact in relation to all security issues on a day-to-day basis, particularly for users.

The Force Accreditor is responsible for the acceptance of information processes and systems connecting to the NYP network. The Force Accreditor acts as an impartial assessor of the residual risk affecting information systems on behalf of the SIRO. If, following the risk assessment, the Force Accreditor determines that the risk is outside NYP's risk appetite statement, the risk is raised to the SIRO for advice and, if necessary, a decision to accept a desired level of residual risk is made. This function is carried out by the ISO.

The Force Vetting Officer is responsible for implementing the NYP vetting process and ensuring (within the parameters set by existing police staff contracts and agreements with police staff unions) that employees, temporary staff and contractors are vetted to an appropriate level determined by their access to NYP's information systems.

The Crypto Custodian is responsible for:

- ensuring the security of NYP's cryptographic assets and encryption key management;
- ensuring that Government policy in respect of cryptographic material is implemented and complied with;
- ensuring that compromise of cryptographic assets is dealt with in line with Government and NYP requirements;

- ensuring cryptographic controls are used in compliance with all relevant agreements, laws and regulations;
- developing and implementing a policy on the use of cryptographic controls for protection of information.

The Information Asset Owner (IAO) is the senior individual responsible for the relevant business area and is responsible for the information process, area of work for which the information system was provided and any approved cloud environment used to deliver the services within the business are and its processes.

The IAO needs to understand what information is held, what is added and what is removed, how information is moved and who has access and why. As a result, the IAO will be able to understand and address risks to the information and ensure that information is fully used with the law for the public good. IAOs will be required to provide a two-yearly assurance statement of the security and use of their assets to support the audit and risk management process. To assist the production of the assurance statement, IAOs should ensure mechanisms are in place to audit permissions access of the storage systems their information is held in and ensure mechanisms are in place to remedy inappropriate access levels. A brief record of permissions auditing should be maintained by IAOs or their nominated representatives. The IAO's will also be required to review their assets in the years between the assurance statements to ensure that their information assets are accurately reflected within the Force documentation and are appropriately protected. This is as per the Information Asset Management process documented within the IAO Handbook.

The IAO is responsible for the establishment and maintenance of relevant security policies for the facilities they own i.e. acceptable use policy, SyOps and ensuring they are available for inclusion in the appropriate documentation.

They are responsible for resourcing and implementing the controls identified in the SyOps but the responsibility for the day-to-day maintenance of these policies and procedures can be delegated to designated System Owners or Information Guardians who manage the systems/information assets at a local level.

In all circumstances, however, the IAO remains ultimately responsible for the security of their information and should be able to determine that any delegated responsibility has been discharged correctly.

ICT Security Governance

To ensure that security is an integral part of information systems, NYP will ensure the following:

- statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls;
- acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance;
- duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of NYP's assets;

- development, test and operational facilities shall be separated to reduce risks of unauthorised access or changes to the operational system;
- when testing systems in a live or test environment, it is preferable to use made up 'dummy' data, or at the very least anonymised data that cannot lead to the identification of an individual;
- authorised and up to date security protection must be installed on any hardware asset connected to the North Yorkshire Police network including any cloud-based service;
- outsourced development of information systems and remote access will be supervised and monitored by NYP in accordance with business and security requirements.

System Owners/Administrators have the delegated responsibility of ensuring the security management of their respective systems including any approved cloud environment.

The System Manager/Administrator is specifically responsible for:

- the maintenance of user accounts from when they first enrol onto the system to when they no longer require access (i.e. creation/amendment/deletion);
- defining access levels for users, in conjunction with the IAO, based on the user's role, 'need-to-know', 'least privileged' and ensuring such profiles are up to date;
- using privileged access workstations for carrying out administrator duties within the IL4 environment;
- ensuring users will only be provided with access to the services that they have been specifically authorised to use;
- re-setting user passwords where necessary, but only when suitably assured of the validity of the request and the identity of the person requesting the reset;
- ensuring that those about to commence work and those currently working on the system have taken the required training;
- checks of the system audit log to ensure the system is being used in line with policies and procedures and that no unauthorised attempt is being made to access the system;
- protective monitoring checks of accounting logs as required to verify relevant information is being recorded and users are using the system correctly;
- ensuring that system patches and updates are applied correctly and in a timely fashion;
- ensuring users are aware of their responsibilities in relation to security when using the system, in conjunction with the ISO;
- identification of any security issues, risks or incidents and the reporting of such to the ISO;
- monitoring of resources and making projections on future capacity requirements to ensure the required system performance;
- ensuring all items of equipment containing storage media shall be checked to ensure any protectively marked information or licensed software has been removed or securely overwritten prior to disposal;
- ensuring the secure and safe disposal of media using formal procedures as contained in Her Majesty's Government (HMG) Information Security Standard 5;
- ensuring, in conjunction with the Information Asset Owner, that users' access rights are reviewed at regular intervals.

To maintain the integrity and availability of information, information processing facilities and all assets and systems including those in any approved cloud environment, Managers/Supervisors have responsibility for ensuring appropriate levels of information security are maintained by their staff and within their areas of work.

Specific responsibilities include:

- supporting the awareness of information security by ensuring staff have sight of this policy and associated procedures;
- ensuring staff complete the necessary e-learning courses for information security such as the Government Security Classification (GSC) Scheme;
- reporting security incidents or potential incidents using the means described in the relevant procedure;
- considering the daily administration of general information security safeguards and countermeasures;
- raising information security issues when appropriate with their Safer Neighbourhood Commander (SNC), Departmental Manager, or where necessary, Head of Function;
- managing updates to local security procedures as and when appropriate;
- providing support for the ISO where necessary i.e. by assisting in monitoring, auditing or inspection exercises as required;
- ensuring authorisation is given to any personnel requiring equipment outside NYP premises;
- ensuring appropriate authentication methods will be used to control access by remote users;
- managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and procedures;
- regularly review their team members' access to systems, data and internet resources, ensuring permissions are set to the required level to suit their role and responsibilities.

Information systems users i.e. all staff and including delivery partners, third party suppliers and contractors with access to NYP's information assets including those in any approved cloud environment, have a responsibility for safeguarding those assets. Every individual using the information systems within NYP must:

- be aware of any relevant practices and protective measures concerning their use of the system to mitigate any risks;
- ensure all information and assets should be treated align with the Government Security Classification (GSC). All users are to complete the relevant information security e-learning courses such as the Government Security Classification (GSC) Scheme;
- use available SharePoint information security resources to build awareness of cyber threats;
- comply with relevant laws, policies rules and standards with regard to information security;
- act safely, sensibly and responsibly in respect of unexpected eventualities;
- draw the attention of management to any relevant issues, circumstances or weaknesses in security arrangements. All suspected security incidents must be recorded on the Security Incident Report accessed via the Force Intranet;
- agree and sign terms and conditions of their employment contract, which confirms their responsibilities for adherence to NYP policies and procedures;
- ensure staff read the FISP upon commencement of employment with NYP;

- ensure that they are permitted to have access to the systems that are required for a business purpose and they are afforded only those privileges that they require access to for their role AND for which they have role responsibilities;
- ensure they use an information system for a policing purpose;
- ensure that the contents of the Policing data should not be passed to any other user or organisation without the specific approval of North Yorkshire Police;
- to prevent unauthorised access to operating systems, NYP will observe the following:
    - access to operation systems shall be controlled by secure log-on procedures; and
    - all users will have a user ID for their personal use only.

Use of Microsoft 365 – the Cloud

NYP users began using Microsoft Office 365 from early 2020 and full rollout took place thereafter. Users will not notice a significant difference in using Exchange Online and in other technologies as the interfaces are similar those users are already familiar with. However, users email domain changed from '@northyorkshire.pnn.police.uk' to '@northyorkshire.police.uk'.

Use of Microsoft Office 365 will fall in line with present policies, procedures and guidance, i.e. the GSC for protective marking will be configured to OFFICIAL and OFFICIAL SENSITIVE.

Use of Cloud based services – excluding Microsoft Office 365

NYP users must not store or transmit NYP information on a cloud computing service unless it has been approved by the Information Security Officer and if necessary, the SIRO. If you are looking to procure a cloud-based service or have been notified that an existing service is moving to a cloud-based platform, please engage with the Information Security team at the earliest opportunity, by contacting them via informationsecurity@northyorkshire.police.uk.

Approval can be obtained through:

- the procurement process and a negotiated contract;
- the implementation of a legal product such as an Information Sharing Agreement or Data Processing Contract; and
- the completion of independent due diligence by the Information Security Officer.

System Access Control

This applies to access to information on applications and/or systems and their functions regardless of the system's hosting i.e. on premises or in the cloud. Users and support personnel shall be restricted in accordance with the defined access control policy. Access to information systems will be role-based and on a 'need to know' basis and in line with the required level of vetting.

Agreements with third parties (including other Forces) and delivery partners, as defined below, involving accessing, processing, communicating or managing NYP's information or information processing facilities, or adding products or services to information processing facilities, shall cover all relevant security requirements. In addition, any delivery partner and/or third party requiring access to NYP's information assets may require one (or more) of the following:

- Information sharing agreement (ISA)

- Data Processing Contract
- Confidentiality Agreement
- Information Systems Access Agreement
- Security Standards Agreement
- Information Security Questionnaire

The access rights to information processing facilities shall be removed on termination of their employment, contract or agreement.

In the scenario where an external user leaves their host organisation, the organisation of the invited guest is responsible for informing the inviting organisation of their users leaving.

The approval for delivery partners/third party supplier access to information systems is ultimately given by the IAO.

Printing
Users must ensure that data is only printed to authorised printing devices and that any protectively marked data is not exposed to any non NYP personnel that may also be working in the same environment i.e. shared premises. Protectively marked information, when printed, must be cleared from printers immediately, appropriately and securely stored when not in use, in line with the Clear Desk and Clear Screen Policy.

Authentication - Passwords
Users of all information systems (network access, applications and smart devices) must ensure they change their passwords in accordance with the password change requirements configured. Users must also follow these points regarding their passwords:

- self-generated passwords must not be easily guessable e.g. ‘password1’ or your surname;
- to prevent this, users must create a strong password, this can be achieved by considering the following:
    - use a mixture of lower and upper case letters;
    - replacing specific letters with numbers e.g. 1 replaces capital I, 3 replaces E;
    - use special characters within your password e.g. !%;
    - use a combination of three random words of minimum 5 characters each
    - do **not** use a password which contains personal information – names, birthdays or dates which are easily related to you;
    - do not use a password which uses keyboard patterns (qwerty) or sequential numbers (12345);
    - if your password has been seen by anyone else it must be changed as soon as possible.
    - passwords must not be shared;
    - passwords must not be disclosed to any other NYP user or unauthorised personnel;
    - if a password compromise is suspected it must be reported immediately to the Information Security Officer and ICT.

- ensure that passwords are not written down or recoded in accessible locations, files or system logs.

Authentication – Biometrics

Smart devices with biometric authentication such as fingerprint and facial recognition may be used to promptly access the smart device for convenience. It is the user's own choice whether to use the technology. Users must remain cautious when using such technology as on occasion, authentication may fail due to angle of finger or face wear. In such cases after three attempts, users will need to use alternative authentication methods such as a fingerprint or password. Users will still need to provide the device nine-digit password if the device has not been authenticated for 24 hours. Users must remain vigilant in using such technology and are asked to consider their surroundings and the safety and security of themselves and the device when considering using the technology. Any security incident must be reported as per the Security Incident Reporting procedure.

Delivery Partner

Delivery partners can fall into two categories, namely:

- Major Delivery Partner - Organisations with which NYP has a significant exchange of protected, personal or business critical information, or holds such information in their own right and where the loss or compromise of that information would impact appreciably on individuals or on NYP; and
- Other Delivery Partner – Any organisation with which NYP either has an exchange of information and uses that information to carry out a business role, or delivers a service on behalf of NYP.

Third Party Supplier

A third party supplier is a commercial entity contracted to supply Information Communication Technology (ICT) and/or related non-ICT services to NYP and includes their suppliers and information/service exchange arrangements e.g. ICT service providers (i.e. where there is a contract in place between NYP and the supplier related to the management of or an exchange of information (Data Processing).

It is the responsibility of NYP to provide assurance that protected personal and business critical data is handled appropriately by its suppliers (and any sub-contractors). Non-ICT service providers could include courier services, document storage or destruction services.

Any third party access to the NYP Microsoft 365 tenancy, inclusive of the different technology stacks, will be assessed and approved through contractual arrangements and/or legal products between NYP and the supplier.

Physical and Environmental Security

Physical security will comply with NYP's Physical Security Procedure.

All staff must ensure that any unauthorised physical access, damage and interference to NYP premises, information and assets is prevented or minimised. This can be done by ensuring the following minimum requirements:

- Windows, doors and any access point are locked when areas are unattended;
- critical, sensitive and/or protectively marked information is protected in secure areas;

- all staff, including uniformed officers, are required to wear visible identification at all times whilst on police premises;
- personnel not wearing visible identification must be challenged.

Further information is available within the Physical Security Procedure.

Visitor Access Control
Visitor access will be strictly controlled. All visitors will be signed into police premises and will be issued with a security pass and a colour-coded lanyard (red indicating they are a visitor).

All staff have the responsibility to provide receptions and front counters with visitors' details and details of the purpose of the visit and who they are there to see. Visitors will have an organisational sponsor who is responsible for managing them whilst on premises and to ensure visitors only access the areas required to fulfil the purpose of their visit.

Clear Desk and Clear Screen Requirements
All staff are required to comply with NYP's Clear Desk and Clear Screen Procedure. The minimum requirements are as follows:

- workstations must be logged off when unattended for long periods and locked (CTRL+ALT+DEL) when left for short periods of time;
- all protectively marked information (including documents etc.) must be locked in a secure environment when unattended;
- All hardware must be locked in a secure environment when unattended.

Communications – voicemail, messaging & faxing
Personnel who fax on a day to day basis or need to leave messages need to be aware as to how and where information and messages are distributed.

- Never fax sensitive information to an unattended fax machine
- Always check the destination fax number before starting your transmission and for sensitive documents contact the intended recipient to ensure the document is immediately collected from the fax machine once transmitted
- Take care with what messages you leave on answer machines and voice mail reducing any protectively marked material

Communications - Email and Internet Use
The email system and access to the internet should be used in accordance with the Internet and Email Procedure. Although access to personal internet services is available through NYP's internet connection, personal internet services are not to be used for the transfer of Police information or for NYP business purposes.

Communications – Secure Communications for postal and email
Sending of organisational communications should be carried out in accordance with the Secure Communications Guidance.

Disposal of Protectively Marked Information
All staff are required to comply with NYP's Protective Marking Procedure. The minimum requirements are as follows:

- protectively marked information e.g. paper files, DVD, CD etc. should be shredded prior to disposal and confidential waste bins used, where provided;
- all items of equipment containing storage media, USB devices, hard drives etc. shall be checked by ISD to ensure that any protectively marked information or licensed software has been removed or securely overwritten prior to disposal;
- ICT ensure the secure and safe disposal of hardware and media using formal procedures as contained in Her Majesty's Government (HMG) Information Security Standard 5.

Disaster Recovery and Business Continuity
A managed process shall be developed and maintained for business continuity throughout NYP, its delivery partners and third party suppliers which addresses the information security requirements needed for NYP's business continuity. All staff are required to comply with NYP's Business Management Continuity Procedure.

Use of hardware and remote working
All staff will only use hardware as procured, configured and provided by NYP. Bring your own device (BYOD) to the organisation for official use is not supported by NYP. Personal devices will not be configured to support NYP communications such as email or NYP evidence capture i.e. images or video footage.

Remote workstations, laptops and any other portable devices such as mobile devices, storage mediums or smart phones are not exempt from this policy.

Further information can be found in the Working with Portable Technology and Documents Procedure.

Protective Marking (Government Security Classifications – GSC)

All staff have a responsibility to ensure that information is protectively marked and handled accordingly and is protected from unauthorised disclosure. This applies to all NYP records and information and must be complied with at all times. All documents that staff create, whether hard copy or electronic format, must carry the appropriate protective marking.

Full details on specific protective marking and handling instructions can be found in the Protective Marking Procedure.

Audit Requirements
All actions by end users and those with elevated administrator permissions are recorded for auditing purposes. All information assets should have auditable trails. The audit trail will include a record of all relevant occurrences. If any significant occurrence is not audited, the whole audit trail can be discredited. As a direct result, all or any information held within the system may also be discredited. For all audit trail data, it will be possible to identify the action, process, enabling hardware and technology used. All transactions will be attributable to a user profile along with the timestamp.

Audit trails will be managed since they may be of critical importance to the organisation. Claims of compliance may be discredited if the audit trail is not treated correctly and cannot be interpreted unambiguously. They should be kept secure and should be available for inspection by authorised personnel.

Linkages
Strategy:
Joint Information and Records Management Strategy

Subsidiary Linked Procedures:
Clear Desk and Clear Screen Procedure
Internet and Email Procedure
Protective Marking Procedure
Working with Portable Technology and Documents Procedure
Security Incident Reporting Procedure
Security Incident Handling Procedure
Physical Security Procedure
Business Continuity Management Procedure
Information Audit Procedure

Other Documents:
HMG Security Policy Framework
Management of police information | College of Policing
Police-Vetting-user-guide