PRINCIPLES DOCUMENT

CYBER SECURITY ARCHITECTURAL PRINCIPLES

ABSTRACT:
This document provides all National Policing and its partners with a clear set of security architectural principles, which are the foundation to build, design and implement secure solutions.

ISSUED	May 2023
PLANNED REVIEW DATE	May 2024
DISTRIBUTION	Policy and Standards Working Group

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

Policy and Standards Working Group should ensure that they are consulting the currently valid version of the documentation.

Document Information

Document Location

PDS - SharePoint\Share\Library\Policy and Forms\

Revision History

Version	Author	Description	Date
v0.1	PDS Police Digtal Service	First draft	15/10/22
V0.2	PDS Police Digtal Service	Updates after initial feedback	15/12/22
V0.3	PDS Police Digtal Service	Further updates and ready draft to submit to Policy & Standards Working Group	24/01/23
V0.4	PDS Police Digtal Service	Responses to feedback from NCPSWG	20/02/23
V0.5	PDS Police Digtal Service	NCPSB Review & approval	23/03/23

Approvals

Version	Name	Role	Date
V0.5	NCPSB	National Cyber Policy & Standards Board	23/03/23
V1.0	PIAB	Police Information Assurance Board	29/06/23

Contents

Document Information 3

Document Location 3

Revision History 3

Approvals 3

Introduction 5

Audience 5

Principles Structure 5

Principles 6

PRINCIPLE 1: Security Fundamentals (Core Security) 6

PRINCIPLE 2: Security by Design 7

PRINCIPLE 3: Segregation and Segmentation 7

PRINCIPLE 4: Virtualisation 7

PRINCIPLE 5: Application Security 8

PRINCIPLE 6: Protective Monitoring 8

PRINCIPLE 7: Automation and Orchestration 9

PRINCIPLE 8: Defend as One 9

Glossary 10

Introduction

Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform, support and prioritise the way in which National Policing decides which ideas, initiatives and/or opportunities are to be progressed (and warrant investment) and those that are not.

Defined security architectural principles should be adopted by security and technical specialists across National Policing. This ensures a consistent approach to the design, development, and implementation of both new and existing solutions that are being refreshed. These security architectural principles cover fundamental security building blocks that must be implemented by default to designed solutions. The security architectural principles focus also on emerging technological concepts that should be used as guidance in conjunction with the National Policing Community Security Principles, National Policing Community Framework, National Policing Community Policy and National DDaT (Digital, Data and Technology) principles.

Audience

This document is intended for a security and technical audience, including, but not limited to security and solution architects across DDaT, PPPT (Police and Public Protection Technology), Home Office and others who contribute to system and network solutions and architectures designs.

Principles Structure

The principles described within this document will be structured in the following way:

Name: Clear, precise and easy to remember.

Statement: Generally, one or two sentences in length. Clearly tells the reader what the principle is.

Rationale: Explanation of why the principle is important and how it will benefit the National Policing and Law Enforcement Organisations.

Implications: Usually in the form of a list to describe what is required to successfully carry out the principle and how it could potentially impact Policing and those who supply to them.

Principles

PRINCIPLE 1: Security Fundamentals (Core Security)

Statement: Solutions and security architects must ensure that core security building blocks are embedded by default into architectural designs to achieve a secure, resilient and well protected environment.

Rationale: Not adhering to core security building blocks will result in core design gaps that could significantly expose network, systems and data to both external and internal threats.

Implications:

- Identity and access management – robust mechanisms must be established to identify, authorise and authenticate users, services and devices and manage their access to sensitive operations, resources and data.
- Confidentiality – unauthorised access to policing data and services must be prevented by designing, documenting and implementing strong people, process and technical controls.
- Integrity – unauthorised modifications to policing data must be detected and prevented to ensure data assurance by designing, documenting and implementing strong people, process and technical controls.
- Availability – policing data and services resilience must be designed-in, implemented and tested to ensure required levels of availability requirements are met. Data and services must be always available for authorised users when they need it.
- Perimeter security – deployed boundary physical and logical mechanisms must effectively detect, prevent and block malicious access attempts to Policing resources and data.
- Endpoint security – all endpoints must be visible and must have proportionate security solutions enabled to detect, block and mitigate malware and malicious activities based on the level of risk that the endpoint exposes organisation to.
- Default Secure – systems must be designed to utilise only required system functionality with unnecessary functionality disabled to minimise attack surface. .
- Data at rest – to ensure data integrity security controls must be proportionate for the value of data being managed.
- Data in transit– data in transit security controls must ensure proportionate end-to-end communication security whether on local networks or over the internet.
- Audit – to ensure policing system have auditing enabled on assets, services and accounts to log necessary events.
- Detect – policing systems must be capable of timely detection of suspicious activity allowing prompt investigation of events. Detection capabilities must be regularly tested and maintained.
- Respond – policing systems must be capable of promptly responding to detected security incidents preventing adversaries' from laterally moving across the networks Incident response plans must be in place and regularly tested.
- Recover – Policing systems must be capable of be promptly restored upon incident allowing continuity of operations. Recovery mechanisms and plans must be in place and regularly tested.
- Decommissioning – all retired assets must be disconnected from the policing systems and securely destroyed. Any data held on assets must be irreversibly and securely erased upon migration to new a system.

PRINCIPLE 2: Security by Design

Statement: Security must be built in from the ground up.

Rationale: The security of our information assets should never be an afterthought. By building security into each phase of the lifecycle of a Policing system, from concept to decommissioning, ensures more effective security, resulting in reduced risk, improved resilience and increased trust across the Policing community.

Implications:

- All new systems will be built following a secure by design methodology.
- National systems will be assured against this principle.
- Information Asset and Risk Owners will need to be engaged throughout the system development lifecycle.

PRINCIPLE 3: Segregation and Segmentation

Statement: Segregation and segmentation is essential to address the complexity of hybrid architectures where each building block of the organisation is independently secured and access verified.

Rationale: Segregation and segmentation mechanisms must be designed and implemented at all layers of the architectural stack to safeguard Policing data and ensure that any identified threats can be effectively contained while Policing continues to operate safely.

Implications:

- All networks and systems must be built with effective physical and logical segregation and segmentation controls across production, development and other environments to restrict access, contain adversaries and minimise the impact of network intrusion. Zero-trust concepts should be followed.
- Systems must be segmented into smaller network segments with strict controls over traffic flowing between different trust zones.
- To protect critical applications, systems and data, effective zoning should be implemented, to minimise the exposure of these systems to external and uncontrolled hostile networks.
- Only security tested and approved versions of the system are promoted into live environments.

PRINCIPLE 4: Virtualisation

Statement: Virtualisation enables Policing organisations to create discrete environments enhancing security, manageability, maintainability and scalability.

Rationale: Implementation of virtualised systems (containerised, virtualised or microservices) and networks by default, enables Policing to adapt more quickly, efficiently and consistently to demands associated with architectural design requirements, supporting rapid deployments of hardened, assured and centrally managed and maintained solutions at scale.

Implications:

- Security and solution architects should prioritise deployment of virtualised technologies aligned with Policing blueprints and best practices.

- Legacy ICT services and applications should be shifted to virtualised technologies that enable enhanced isolation, security and recovery.
- Policing will deploy consistent virtualised technologies to enhance maintenance, administration and cost efficiency while ensuring higher level of security.
- Virtualised operating systems and applications should be properly isolated to minimise the attack surface.

PRINCIPLE 5: Application Security

Statement: Application security and privacy must be executed at all phases of the software development life cycle.

Rationale: By building application security into each phase of the software development life cycle of a Policing system, it encourages developers to build highly secure software, addresses compliance requirements, and reduces development costs, resulting in reduced risk, improved resilience and increased trust across the Policing community.

Implications:

- Strong software development life cycle (SDLC) governance must be adopted.
- Standardisation across Policing applications development must be embraced by utilising approved and formalised SDLC standards and frameworks to ensure high standards of software.
- A comprehensive review of the application code to identify any vulnerabilities introduced as a result of coding errors.
- Regular testing should be conducted against known weaknesses and vulnerabilities using industry standard testing methodologies / frameworks to ensure security is maintained.
- Centralised catalogue of secure APIs (Application Programming Interface) and third-party applications will ensure comprehensive, consistent and secure API sets and software for partners and forces.
- Safeguarding applications with ICT security technologies and services ensures enhanced protection of Policing system against known and unknown threats.

PRINCIPLE 6: Protective Monitoring

Statement: Policing cannot defend what they cannot see. Policing systems must be built with protective identification and monitoring capabilities by design.

Rationale: Security logging and monitoring is central to the identification and detection of threats. This allows forces to establish and understand the baseline patterns of activities across policing systems, which in turn provide indicators of compromise, allowing response and recovery from incidents in timely manner.

Implications:

- Auditing by design concept must be built into all new Policing systems to ensure accountabilities for all devices, services and network communication.
- Effective intrusion detection requires multiple sources of information.
- Architects, security engineers, Information asset owners and the National Management Centre (NMC) will need to be engaged to collectively identify and establish sensitive events that must be audited.

- Comprehensive and regularly tested incident plans must be in place, maintained and tested for information security events.
- Continuous monitoring of all assets is required with 24 by 7 coverage.

PRINCIPLE 7: Automation and Orchestration

Statement: Architects and security engineers will employ an automation strategy to enable Policing to sustain itself and support missions while orchestrating and automating systems, network and security wide operations.

Rationale: Embedding an orchestration and automation strategy across Policing will significantly boost Policing's cyber security posture by enabling security, system and network tools to work together to streamline security processes and completion of tasks without human intervention. As a result, this will allow forces and the National Management Centre to reduce operational security overheads while maximising efforts to respond to threats.

Implications:

- New systems and solutions should be designed to allow seamless integration with orchestration and automation tools as well as National Management Centre SIEM.
- Self-learning and autonomous cyber solutions should complement and enhance the current security controls to protect assets, processes and employees at every layer of the architectural stack.
- Regular evaluation should be conducted to ensure Security, Orchestration, Automation and Response (SOAR) capabilities are maintained.

PRINCIPLE 8: Defend as One

Statement: Collective and coordinated cyber operational engagement across National Policing must be undertaken to fight emerging threats at scale.

Rationale: By combining cyber abilities, expertise and threat intelligence in coordinated approach, National Policing amplifies cyber security operational capabilities to combat and defend against continuously evolving threats at scale while ensuring cost effectiveness and security efficiency.

Implications:

- National Policing will embrace and align with the Defend as One approach.
- Incident Management solutions and designs should be integrated with the offerings of the National Management Centre.
- Policing systems should be designed to allow collaborative and seamless data sharing between Information Asset and Risk owners across all Policing forces.
- Policing solutions should be designed collaboratively, built once, and centrally coordinated allowing forces to implement consistent, well integrated and assured systems.

Glossary

Segregation and segmentation: is security best practice that allows to achieve break up points between different resources from other parts of the organization with strong, more granular controls and processes to effectively prevent, detect and contain adversary movements across segments. Segregation and segmentation is typically achieved across, but not limited to, solutions, systems, networks, applications, functions or teams. Segregation and segmentation are key to achieve Zero Trust design.