CYBER GUIDELINE DOCUMENT

Information Compliance using Microsoft Purview

ABSTRACT:
This guidance describes best practice for monitoring, auditing and assuring the Office 365 tenancy minimise the risk to policing information within the Microsoft 365 service.

ISSUED	March 2024
PLANNED REVIEW DATE	February 2025
DISTRIBUTION	Community Security Policy Framework Members

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

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

CONTENTS

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 guideline in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing requirements for information assurance.

Introduction

Policing organisations' Microsoft Office 365 environments are assured to process OFFICIAL SENSITIVE Policing data through the PDS blueprint designs complemented by the Security Assessment for Policing (SyAP). Their development, configuration and assurance status are a continuous cycle to ensure its performance, health and security are within the national and organisational risk appetite. Microsoft environments are protected through external protective monitoring. The internal capabilities of the tenancy and network should be subject to internal assurance activity to evidence its confidentiality, integrity and availability. This can be achieved through Information Management (IM) policy, incident reporting, monitoring / auditing, reporting and risk analysis. The value of such activity complements the continuous assurance of the tenancy alongside the tenancy configuration patterns, testing and supports the local organisation to view and improve their compliance position, rating and maturity requirements.

For the purposes of this document, "Purview" refers to Microsoft Office's compliance manager solution.

This guidance document includes assurance activity to minimise the risk to policing information whilst the critical Microsoft Office 365 service is operational.

This guidance is written on the assumption that environments are compliant to the latest PDS blueprint design. Furthermore, it is assumed police forces have deployed appropriate licences as directed under the Memorandum of Understanding. Some capabilities are not available under the E3 licencing. This guidance will offer recommendations beyond the blueprint designs I.e., if a police force has matured in creating further IM based policies and corporate functional work flows I.e. use of eDiscovery in their environment which will provide evidence of maturity. This guidance does NOT exhaust and cover all capabilities of Purview. A police force is encouraged and welcomed to develop the capabilities of their environments beyond this document within the full capabilities of their licensing ensuring that the scopes monitored, audited and reported are documented.

Owner

National Chief Information Security Officer (NCISO).

Purpose

Ensure that policing information processed with the Microsoft Office 365 tenancy by the organisation and individuals is protected, used for a business and policing purpose and compliant with National and local security requirements.

Audience

This guidance is aimed at:

- Force / organisational Senior Information Risk Owners (SIROs),
- Information Governance Managers,
- Data Protection Officers (DPOs),
- Records Managers (RM),
- Information Security Officers (ISOs),
- Information Security practitioners,
- Information Asset Owners (IAOs),
- Information Technology Security Officers,
- Security Engineers/Analysts
- Professional Standard Branches (PSB) / Anti-Corruption Unit (ACU) officers.

Scope

This guidance applies to any member of the Policing Community of Trust in a compliance and professional conduct-based role accessing Purview to manage Information Management agendas. This guideline is focussed on assurance activity to be conducted by the organisation to protect the inner processing of the tenancy against national and local security and assurance requirements.
Policing information assets and applications which operate with them throughout their lifecycle such as;

1. Information creation and editing tools (Microsoft Office applications for example)
2. Information communication tools such as electronic mail and messaging tools
3. Collaboration tools, intranet / Microsoft SharePoint for example
4. Databases and data repositories
5. Application development solutions
6. Information storage solutions

Requirements

Reference	Minimum requirement	SyAp Control and baseline pattern reference (if relevant)
1	**General**	
1.1	In line with local policies, Information compliance, Security and professional conduct-based roles are mapped to appropriate roles within a Privileged Identity Management (PIM) solution. The organisational access control and or equivalent policy deploys the operational process for PIM including how roles are applied for, approved, audited and document local decisions I.e., length of time privilege can be escalated).	PR.AC-1 and 4, PR.AT-2, PR.PT-3 Baseline pattern IAM and PS Vol 2, section 2.6.

Reference	Minimum requirement	SyAp Control and baseline pattern reference (if relevant)
2	**Risk Assessment** A full risk assessment must be documented, to include:	
2.1	A critical environment level security risk and assurance document for Microsoft Office 365. As required through the Security Assessment for Policing (SyAP) control ID.GV.4. Providing a local roles and responsibilities definition against PIM based roles and their assurance activities. For example, PSB/ACU conducting research and analysis through eDiscovery. Furthermore, scopes of IM and assurance auditing, metrics and reporting structures.	ID.GV-2/4, DE.DP-1, ID.BE-4, ID.GV-4 and ID.RM-1
2.2	Mechanisms of referring IM and security auditing into potential professional conduct, personal data breaches and or security incidents.	PR.PT-1
2.3	Scopes of IM and security auditing (this guidance document) which assure the environments usage against the organisation's risk appetite.	PR.PT-1
2.4	What metrics, management information and compliance assessment (SyAP and present architectural pattern compliance and roadmap) are analysed, escalated and used as a baseline I.e. compliance status against National Office 365 patterns for up to OFFICIAL SENSITIVE.	ID.GV-3
2.5	Organisation to define how metrics are reported, where and to whom. I.e. what board and how is it presented?	ID.GV-4, PR.AT-4

Reference	Minimum requirement	SyAp Control and baseline pattern reference (if relevant)
3	**Purview – Compliance Manager solutions – App Governance**. Helps you understand all applications that connect to your organization and govern their API activity.	
3.1	Police force to register all third parties' applications connected to their tenancy in the Information Asset Register, ensuring all due diligence against the integration is complete, risk assessed and documented as per their local third-party assurance procedures.	DE.CM-6, ID.AM-4 and ID.SC-2
3.2	Create a local workflow for security-based roles and functions to receive, monitor, analyse and respond to detection alerts. Using remediation to contain issues automatically where possible.	PR.DS-6
3.3	Organisation to define what Insights and detection metrics are reported as a standing item to the IM based board, Security, Microsoft Office or equivalent board.	ID.GV-4, PR.AT-4
4	**Purview – Compliance Manager solutions – Data lifecycle management**. Manages your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't. **Purview – Compliance Manager solutions – Records Management**. Uses intelligent classification to automate and simplify the retention schedule for regulatory, legal, and business-critical records in your organization.	
4.1	In line with local records retention policy and from baseline designs support; create local retention policies for Exchange (including group mailboxes and archiving), Sharepoint Online, PowerApps, Forms, One Drive and Teams. Review and develop local records management and security-based policies and workflows to notify and	PR.IP-6 Baseline pattern IAM and PS Vol 3, section 6.3.

Reference	Minimum requirement	SyAp Control and baseline pattern reference (if relevant)
	guide users particularly if users are empowered to select own retention label and or have exceptions for further periods. Consultation with Data Protection and Records Management governance nationally maybe required.	
4.2	Create a local workflow for records management-based roles and functions to receive, monitor, analyse and respond to inactive mailboxes. Schedule a three-monthly audit to ensure inactive mailboxes stands to scrutiny against the organisational Joiners, Movers and Leavers (JML) policy.	PR.IP-11
4.3	Organisation to define what audit output and mailbox metrics are reported i.e. volume in each state i.e. LIVE and ARCHIVED) as a standing item to the IM, Office 365 or equivalent board.	ID.GV-4, PR.AC-4, PR.PT-1
4.4	Organisation to direct on under what circumstances, authority level and process is required for archiving mailboxes (if they have any requirement), in alignment with the JML policy. Workflow to be created to manage requests through local Information Asset Owners and the records management function.	PR.IP-11 Baseline pattern IAM and PS Vol 3 - DR3-DG03.
5	**Purview – Compliance Manager solutions – Data Loss Prevention (DLP)**. Detects sensitive content as it's used and shared throughout your organization, in the cloud and on devices, and helps prevent accidental data loss. If the Police force have created additional DLP policies. Such will form part of the audit scope.	

Reference	Minimum requirement	SyAp Control and baseline pattern reference (if relevant)
5.1	Create a local workflow for security-based roles and functions to receive, monitor, analyse and respond to DLP alerts.	RS.CO-2, RS.MI-1 and 2 Baseline pattern IAM and PS Vol 3 – 6.2.2.11.
5.2	Management of, and response to, alerts to be based on their severity level. Contain, record, investigate, educate, remediate and or refer for PSB/ACU involvement.	PR.PT-1 Baseline pattern IAM and PS Vol 3 – 6.2.2.11
5.3	Organisation to define what audit output and DLP metrics are reported as a standing item to the IM, Office 365 or equivalent board.	ID.GV-4, PR.AC-4
6	**Purview – Compliance Manager solutions – Information Protection**. Discovers, classifies, and protects sensitive and business-critical content throughout its lifecycle across your organisation. Ensure the organisation is using data classification correctly and protecting the confidentiality of communications as per organisational policy.	
6.1	Management of, and response to, alerts to be based on their severity level. In addition, schedule a three-monthly audit of data classification covering communications in exchange (including use of 'encrypt' and 'do not forward') teams, Sharepoint and the Power Platform and, documentation classification. Contain, record, investigate, educate, remediate and or refer for PSB/ACU involvement.	ID.AM-6, PR.PT-1, RS.MI-1 and 2
6.2	Organisation to define what audit output and data classification metrics are reported as a standing item to the IM, Office365 or equivalent board.	ID.GV-4, PR.AC-4

Reference	Minimum requirement	SyAp Control and baseline pattern reference (if relevant)
6.3	Organisation to determine security responsibilities in policy/procedures for Microsoft 365 for Teams, Sharepoint and the Power Platform applications owners and administrators. I.e., permission management, JML and business usage.	PR.IP-11
6.4	Schedule a three-monthly audit of Sharepoint Information Rights Management (IRM). Scoping including permission changes, JML and document challenges of site owners.	PR.IP-11, PR.PT-1
6.5	Schedule a three-monthly audit of Teams permissions changes, JML and document challenges of team owners.	PR.IP-11, PR.PT-1
6.6	Microsoft 365 Defender. Cloud Access Security Broker (CASB) that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services:	
6.7	Update incident management policies, directives and workflows to include the requirement to manage active incidents and alerts in defender – incidents and alerts. Management and response to alerts to be based on their severity level.	DE.AE-2, RS.CO-2, RS.MI-1 and 2. RS.MI-3
6.8	Threat analytics from Microsoft Defender and National Management Centre reported as a standing item to the IM, Security, Office365 or equivalent board.	DE.CM-7, ID.RA-2/4/5, PR.DS-4

Reference	Minimum requirement	SyAp Control and baseline pattern reference (if relevant)
6.9	Microsoft secure score metrics from the reports section – identify, data, devices and apps. Report as a standing item to the IM, Security, Office365 or equivalent board Manage and distribute maturity requirements to minimise local risks and to keep the risk appetite at the organisational acceptable level. Providing evidence for the SyAP.	ID.GV-4, ID.RA-1, PR.AC-7, PR.AC-4, PR.IP-3, PR.IP-7, PR.MA-1
7	**Purview – Compliance Manager solutions – Communications compliance and Information barriers**. Minimizes communication risks by helping you automatically capture inappropriate messages, investigate possible policy violations, and take steps to minimize harm. Allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint Online, and OneDrive for Business.	
7.1	Review what policies are needed in the organisation. Create relevant policies within the communications compliance solution against security and professional conduct based corporate policies and directives within the organisation. Policies must be aligned with corporate requirements and within the organisations risk appetite.	DE.CM-3, ID.GV-2
7.2	Create a workflow to manage the policy to use proactively and reactively to circumstances. Workflow to define the roles and responsibilities between the security and professional conduct-based functions within the organisation. Defining an appropriate detection, investigation, containment, remediation, recording and referral processes. Organisation to consider capabilities of 'Information barriers' and to corporately decide on its deployment	RS.CO-2, RS.MI-1 and 2. RS.MI-3

Reference	Minimum requirement	SyAp Control and baseline pattern reference (if relevant)
	against their maturity and assessment of necessary and proportionality.	
7.3	Organisation to define what audit output and metrics are reported as a standing items appropriate (confidential) boards and other governance reporting mechanisms locally deployed.	ID.GV-4, PR.AC-4, PR.PT-1
8	**Purview – Compliance Manager solutions – Insider Risk Management – Insider risk management**. Available through E5 licence only. Detect risky activity across your organization to help you quickly identify, investigate, and act on insider risks and threats.	
8.1	Review what policies are needed. Create relevant policies within the Insider Risk Management solution against security and professional conduct based corporate policies and directives within the organisation. Policies must be within the organisation's risk appetite for example with data theft, security policy violations and data leaks.	ID.AM-6, RS.MI-1 and 2
8.2	Create a workflow to manage the policies to use proactively and reactively to circumstances, as appropriate. Use the user activities as proportionate to investigate, respond and monitor activity; I.e., (not exhaustive list) delete sensitivity labels, deletes files, send sensitive message, unusual amounts of downloads, copy files to USB etc. Workflow to define the roles and responsibilities between the security and professional conduct-based functions within the organisation. Defining an appropriate detection, investigation, containment, remediation, recording and referral processes.	PR.DS-5, RS.CO-2, RS.MI-3

Reference	Minimum requirement	SyAp Control and baseline pattern reference (if relevant)
8.3	Organisation to define what audit output and relevant metrics are reported as a standing items to appropriate (confidential) boards and other governance reporting mechanisms locally deployed.	ID.GV-4, PR.AC-4, PR.PT-1
9	**Purview – Compliance Manager solutions – Discovery and response section – Audit**. Records user and admin activity from your organization so you can search the audit log and investigate a comprehensive list of activities across all locations and services. eDiscovery Searches across content locations to identify, preserve, and export data in response to legal discovery requests and eDiscovery cases.	
9.1	Organisation to review and update their professional conduct and security-based policies and directives to ensure business monitoring reflects the capabilities of Office 365.	ID.AM-6, ID.GV-2, RS.MI-1 and 2
9.2	Create a workflow to manage the usage of the audit capability define when it is appropriate and necessary to audit policies to use proactively and reactively to circumstances as appropriate. Use the user activities as proportionate to investigate, respond and monitor activity; I.e., (not exhaustive list) delete sensitivity labels, deletes files, send sensitive message, unusual amounts of downloads, copy files to USB etc. Workflow to define the roles and responsibilities between the security and professional conduct-based functions within the organisation. Defining an appropriate detection, investigation, containment, remediation, recording and referral processes.	RS.CO-2
9.3	Organisation to define what audit output and relevant metrics are reported as a standing items appropriate (confidential) boards and other governance reporting mechanisms locally deployed.	ID.GV-4, PR.AC-4, PR.PT-1

Reference	Minimum requirement	SyAp Control and baseline pattern reference (if relevant)
10	**Purview – Compliance Manager solutions – Discovery and response section – Data subject requests**. Finds and exports a user's personal data to help you respond to data subject requests for GDPR.	
10.1	Organisation to review and update their Data Protection, Subject Rights and professional conduct / business monitoring directives to include Office 365 capabilities.	
10.2	Create a workflow to manage the usage of the eDiscovery function for professional conduct, security and Data Protection requirements. Detail to include when it is appropriate and necessary to use the solution proactively and reactively.	RS.CO-2, RS.MI-1 and 2
10.3	Organisation to define what audit output and relevant metrics are reported as a standing items appropriate (confidential) boards and other governance reporting mechanisms locally deployed.	ID.GV-4, PR.AC-4, PR.PT-1

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.
- 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 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.

This document should be available to key stakeholders including SIRO, IAO's, Information Security Officer, Human Resources, Professional Standards, Records Management, Data Protection Officers, Operational Leads, and the senior managers of Force areas which may incur travel. Additionally, the Force ICT department should be aware of this guideline.

Review Cycle

This guideline 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 guideline 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

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	PDS Cyber	Initial version	01/06/2023
0.2	PDS Cyber	Revision	29/02/2024

Approvals

Version	Name	Role	Date
1.0	NCPSWG	National Cyber Policy & Standards Working Group	06/03/2024

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2022	07/2022
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
Authorised Professional Practice on Information Assurance	Jun 2020	16/06/2020
National Policing Information Risk Appetite	As published	01/01/2012
Security Awareness in Fragile Environments (SAFE) – UK Government Security	As published	Online resource
Open-source diagram for Microsoft Office 365 Licensing map	As published	Online resource
Open-source Microsoft 365 – feature matrix	As published	Online resource
Microsoft at their compliance and risk resources.	As published	Online resource