CYBER GUIDELINE DOCUMENT

NCSP Guideline – Microsoft Power Platform

ABSTRACT:
This guidance is to assist members of the UK policing community of trust in the design, setup and use of Microsoft's Power Platform service, incorporating Power Apps, Power Automate, and Power Pages

ISSUED	October 2024
PLANNED REVIEW DATE	October 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 guidelines for the use of Microsoft Power Platform.

Introduction

This guidance is to assist members of the UK policing community of trust in the design, setup and use of Microsoft's Power Platform service, incorporating Power Apps, Power Automate, and Power Pages. Dataverse is also briefly covered due to how it interacts with the other components. It does not cover Copilot Studio (formerly Power Virtual Agents) due the rapidly changing nature of this component.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this guideline is to provide members of the policing community of trust with a reference guide to help them design the deployment of Power Platform, to build it and build on it in a secure manner and manage the lifecycle of the platform and the applications built on it.

Audience

"security is a complex article and is best accomplished as a joint effort between application makers and the team administering user permissions"[1]

This guidance is for staff members within National Policing and its community, who will be leading the implementation and ongoing management of Power Platform within their environments.

Further, this guidance should also be read by those who are developing applications and processes on top of the Power Platform to ensure that said applications and processes are built in a secure fashion.

[1] MS: Security concepts in Dataverse

Scope

1. This guidance should be adopted by all policing organisations using Power Platform.
2. This guidance should be followed by all those charged with creating and managing Power Platform environments.
3. This guidance should be followed by all those who create and manage applications and processes built on Power Platform.

Requirements

"Start from now with evaluation. It's not too late. Gaps can either be accepted, or remediated."[2]

Reference	Minimum requirement	Control reference
1.	**Core**	
1.1	Ensure the necessary licenses are in place before starting.	IAM & PDS Blueprints, volume 4, section 6.3
1.2	Have an organisational plan or strategy on what Power Platform should be used for. Build and license it appropriately.	SOGP SG1.2.2 MS: Develop a tenant strategy to adopt PP at scale
1.3	Consider using the "Power Platform adoption maturity model" to build a roadmap.	MS: Develop a tenant strategy to adopt PP at scale
1.4	Have a written policy for the use of connectors and libraries.	OWASP Low-Code/No-Code Top 10: 7 SOGP SG1.1 SOGP IR1.2.2
1.5	Information security policies should cover no-code/low-code development.	SOGP SM1.1.3
1.6	Use organisational risk appetite to define necessary controls.	SOGP SG1.3.3
1.7	Consider an acceptable use policy for developers.	SOGP SM1.2.1
1.8	Prefer native tooling, for Power Platform administration, rather than custom tools.	MS: Develop a tenant strategy to adopt PP at scale

[2] MS: Develop a tenant strategy to adopt Power Platform at scale

Reference	Minimum requirement	Control reference
1.9	Note that each environment starts with 1GB of storage that is shared with all items in it.	MS: Develop a tenant strategy to adopt PP at scale
1.10	A high-level security architecture should be created to cover various usages.	SOGP TI2.1.1
1.11	Apply zero-trust principles.	SOGP TI2.2.1
1.12	Monitor application load in relation to the platform service levels and license limits.	SOGP SR1.4.1
1.13	Consider security testing of higher risk, or higher privilege apps, and any environment controls to ensure intended configuration is met.	SOGP AS1.2.1 SOGP UA2.1.8
1.14	Use Privileged Identity Manager for administrative actions.	IAM & PS Blueprints, volume 4, section 6.4.8 MS: Use Service Admin roles to manage your tenant
1.15	Test changes before deploying to live environments.	SOGP SR1.3.2
1.16	Enable cross-tenant isolation.	CIS Microsoft Dynamics 365 Power Platform: 2.5
1.17	Service principals over service accounts.	IAM & PS Blueprints, volume 4, section 6 IAM & PS Blueprints, volume 4, section 6.1 IAM & PS Blueprints, volume 2, section 2.3.4.1.5 OWASP Low-Code/No-Code Top 10: 1 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 1
2.	**Features**	
2.1	Turn off trial licensing.	IAM & PS Blueprints, volume 4, section 6.4.1

Reference	Minimum requirement	Control reference
2.2	Turn off self-service purchasing.	IAM & PS Blueprints, volume 4, section 6.4.2
2.3	Track the development and release of new platform features via the official Microsoft roadmap.	MS: Develop a tenant strategy to adopt PP at scale
3.	**Tracking developments**	
3.1	Document business critical apps in an asset register, including who owns it.	SOGP AM1.1.2 SOGP AM1.1.3 SOGP UA2.1.5
3.2	An asset owner should be appointed for the platform, and for each app that is developed on it.	SOGP AM1.2.1
3.3	Create internal service agreements for developed applications.	SOGP SR1.1.3 SOGP SR1.1.7
3.4	Maintain a Software Bill of Materials (SBOM).	OWASP Low-Code/No-Code Top 10: 7 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 7
4.	**Lifecycle**	
4.1	Consider using CI/CD pipelines for promoting solutions from development to production environments.	MS: Develop a tenant strategy to adopt PP at scale SOGP SD1.3.1
4.2	If moving solutions between tenants (i.e. if using separate tenants for dev/prod rather than environments), consider using built in or locally / nationally assured software version control such as Azure DevOps or GitHub.	MS: Develop a tenant strategy to adopt PP at scale
4.3	Make use of application reviews to ensure best practices are being followed.	Microsoft Internal Security Best Practices: Secure Power Platform Development
4.4	Use Sandboxes for testing.	IAM & PS Blueprints, volume 4, section 6.4.5

Reference	Minimum requirement	Control reference
4.5	Track configuration changes to the environment and to applications built on it.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 5 SOGP SR1.3.1
5.	**Data loss prevention**	
5.1	Use DLP policies at either the tenant or environment levels.	IAM & PS Blueprints, volume 4, section 6.4.3 OWASP Low-Code/No-Code Top 10: 3 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 3 MS: Secure the default environment MS: Develop a tenant strategy to adopt PP at scale SOGP IM1.6.1 CISA Power Platform Secure Cloud Business Applications: 4.1.1
5.2	Use DLP policies to restrict the connectors that can be used.	CIS Microsoft Dynamics 365 Power Platform: 3.4 OWASP Low-Code/No-Code Top 10: 3 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 3 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 7 MS: Secure the default environment

Reference	Minimum requirement	Control reference
5.3	All environments should have at least one DLP policy applied.	CISA Power Platform Secure Cloud Business Applications: 4.1.2
5.4	In the DLP policies, set a custom message to steer users towards a central compliance team.	MS: Secure the default environment
5.5	Consider an "ultra low" DLP policy for the default environment, which provides only the bare minimum needed for Dataverse and notifications.	Microsoft Internal Security Best Practices: Secure Power Platform Development
5.6	Set new connectors to the "blocked" category so it cannot be used until approved.	IAM & PS Blueprints, volume 4, section 6.4.3 MS: Secure the default environment SOGP SD1.4.2
5.7	For apps/connectors that have been assured for use, add them to a "low" or "medium" policy.	Microsoft Internal Security Best Practices: Secure Power Platform Development
5.8	Think carefully about allowing "HTTP", "HTTP with AAD" and "HTTP Webhook" as they could be used to leak data.	Microsoft Internal Security Best Practices: Secure Power Platform Development
5.9	Limit creation of custom connectors to approved and competent developers.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 3 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 4 MS: Secure the default environment
5.10	Any custom API's should be created securely.	SOGP TI1.2.6
5.11	Consider app reviews to ensure suitable DLP coverage.	OWASP Low-Code/No-Code Top 10: 3
5.12	For connectors that have "endpoint filtering", like the connector for MS SQL Server, consider configuring it to grant/deny access by FQDN, IP address, or pattern matching.	Microsoft Internal Security Best Practices: Secure Power Platform Development

Reference	Minimum requirement	Control reference
5.13	If you wish to block the ability to send emails, use rules in Exchange which checks the user agent in the SMTP header.	MS: Secure the default environment
5.14	Limit data extraction permissions.	CIS Microsoft Dynamics 365 Power Platform: 3.2
5.15	Set the blocked file types list to match the corporate standard.	CIS Microsoft Dynamics 365 Power Platform: 2.3
6.	**Audit and compliance**	
6.1	Apply monitoring for audit, compliance and security.	IAM & PS Blueprints, volume 4, section 6.4.9
6.2	Log environment activity, with retention in line with corporate logging policy.	CIS Microsoft Dynamics 365 Power Platform: 4.2 OWASP Low-Code/No-Code Top 10: 10 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 10
6.3	Make use of the M365 Security and Compliance Centre for audit and monitoring of the platform and apps.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 1 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 3
6.4	Make use of the MS Purview for audit and monitoring of the platform and apps.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 2 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 3
6.5a	Note that logging of admin logs to Purview is on by default, but E5 licenses are needed to access it.	MS: View PP admin logs using auditing solutions in MS Purview

Reference	Minimum requirement	Control reference
6.6	Implement custom logging if the built-in logging is insufficient for your needs.	OWASP Low-Code/No-Code Top 10: 10 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 10
6.7	Ensure no sensitive data is written to logs.	OWASP Low-Code/No-Code Top 10: 10 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 10
6.8	Consider alerting for app creation.	CIS Microsoft Dynamics 365 Power Platform: 4.3
6.9	Use Power Automate Admin and Management connectors to build automations to monitor the PP environment.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 1 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 3
6.10	Disable or monitor use of shared connectors – as appropriate to the environment.	OWASP Low-Code/No-Code Top 10: 2
7.	**Sharing of apps and connectors**	
7.1	Consider limits on who the app can be shared with.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 1
7.2	Consider limits on sharing of Flows.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 2
7.3	If sharing Flows with other co-owners, check which accounts are used by connectors.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 2
7.4	Deny anonymous access unless explicitly needed, after a risk assessment, which has been recorded, mitigated, and approved by the relevant IAO(s), after consultation with the ISO.	OWASP Low-Code/No-Code Top 10: 5
8.	**Developers**	

Reference	Minimum requirement	Control reference
8.1	Educate developers on the implications of connector selection and configuration.	OWASP Low-Code/No-Code Top 10: 2
8.2	Educate developers on implications of not validating user input.	OWASP Low-Code/No-Code Top 10: 6 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 6 SOGP BA1.4.1
8.3	Use MS Learn modules as part of a programme to educate developers.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 2 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 4 SOGP AC1.4.5
8.4	Train developers in security processes.	SOGP ST1.1.1
8.5	Critical apps should be developed by those trained in security techniques and methodologies.	SOGP UA2.1.1
9.	**Good practices**	
9.1	Do not hard code secrets, tokens, or other sensitive values.	OWASP Low-Code/No-Code Top 10: 8 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 8 SOGP SD3.1.7
9.2	Protect sensitive fields so they cannot be viewed or otherwise accessed by those without appropriate privileges.	SOGP SD3.1.7
9.3	Monitor code for sensitive values being hardcoded.	OWASP Low-Code/No-Code Top 10: 8 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 8

Reference	Minimum requirement	Control reference
9.4	Inventory all user developed apps, including users, owner, and agreed service levels.	OWASP Low-Code/No-Code Top 10: 9 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 9
9.5	Have a plan for migration of ownership of apps for when owners leave or change roles.	OWASP Low-Code/No-Code Top 10: 9
9.6	Have a process in place for support and maintenance, removing single points of failure by ensuring sufficient coverage for those on leave, sick or no longer employed.	SOGP UA2.1.11
9.7	Apply least privilege principles for access to business data (using predefined security roles where they exist).	CIS Microsoft Dynamics 365 Power Platform: 2.2 OWASP Low-Code/No-Code Top 10: 1 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 1 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 2 SOGP AC1.1.2
9.8	Do not rely on filtering or other client-side controls for security.	MS: Use of MSSQL with PP
9.9	Do not disable control elements (in Power Apps) as a security measure.	Microsoft Power Platform Security FAQs
9.10	Use "secure implicit connections" for database connectors.	MS: Use of MSSQL with PP
9.11	Revoke DB connections that are not "secure implicit connections".	MS: Use of MSSQL with PP Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 2

Reference	Minimum requirement	Control reference
9.12	Apply careful consideration around which accounts or principals are used for each connector.	OWASP Low-Code/No-Code Top 10: 2
9.13	Use query parameterisation and stored procedures where possible.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 6
9.14	Consider Content Security Policy (CSP) for canvas and model apps.	Microsoft Content Security Policy for Power Platform
10.	**Risk management**	
10.1	Make use of Sensitivity Labels to ensure the marking of any output is marked respective to its input(s).	Microsoft Internal Security Best Practices: Secure Power Platform Development SOGP IM1.3.3 SOGP IM1.3.7
10.2	For apps working with data, conduct information risk assessments.	SOGP IR1.2.3
10.3	For business-critical apps, conduct information risk assessments, with any findings addressed and signed off by the relevant IAO(s) after consultation with the ISO.	SOGP IR1.2.6 SOGP UA2.1.6
10.4	For enterprise apps, information risk management activities should take place.	SOGP IR1.1.11
10.5	Conduct a business impact assessment to assess the impact of any compromise of confidentiality, integrity and availability.	SOGP IR2.2.4
10.6	Consider threats from low-skilled developers and what mitigations/controls are needed.	SOGP IR2.3.3
10.7	Protect apps with regular backups and controlling access and changes to source code.	SOGP UA2.2.5
10.8	Consider exporting solutions to an offline backup periodically.	SOGP SR1.5.2
11.	**Power Pages**	

Reference	Minimum requirement	Control reference
11.1	Web roles can be used for special actions or for access to protected content, by linking users to table and/or page permissions.	MS: Power Pages Security
11.2	Users can be allocated multiple web roles, allowing cumulative access.	MS: Power Pages Security
11.3	Users who have been authenticated are automatically added to "Authenticated Users" role.	MS: Power Pages Security
11.4	Users who are not authenticated are automatically allocated to the "Anonymous Users" role.	MS: Power Pages Security
11.5	Use table permissions to control access to Dataverse content such as lists, forms, liquid, and the web API.	MS: Power Pages Security
11.6	Use page permissions to control access to whole pages and/or to specific elements on pages.	MS: Power Pages Security
11.7	Consider configuring the CORS header to control cross-origin requests.	MS: Power Pages Security MS: Power Pages Security Whitepaper
11.8	Consider configuring the X-Frame-Options-Header, X-Content-Type-Options, and Content Security Policy.	MS: Power Pages Security Whitepaper
11.9	Make use of "Security Scan" to check for common threats like cross-site-scripting, and use of insecure libraries.	MS: Power Pages Security
11.10	Use "Portal Checker" to check for common site configuration issues.	MS: Power Pages Security Whitepaper
11.11	If you wish to use the built-in WAF, you will also need to turn on the Content Delivery Network (CDN). This may cause data-residency issues so should be used after consideration of the data being delivered by the Power Pages site.	MS: Configure WAF for Power Pages SOGP BA1.3.1 SOGP BA1.3.4 SOGP CA1.2.2
11.12	If using the CDN, static content is cached at global points-of-presence, but the default list of content types can be altered on a per site basis.	MS: Configure WAF for Power Pages

Reference	Minimum requirement	Control reference
11.13	Changes to site visibility have immediate effect so care should be taken to ensure the suitability and integrity of any sites that are moved from private to public.	MS: Site Visibility in Power Platform
11.14	Sites in developer environments cannot be made public.	MS: Site Visibility in Power Platform
11.15	Private sites can be accessed by the owners, and authenticated internal individuals (via Entra ID), but only up to 50 users.	MS: Site Visibility in Power Platform
11.16	Site visibility can be changed by holders of various privileged roles, such as Global Admin, Power Platform Admin, Dynamics 365 Admin, or can be delegated by changing the "enableSystemAdminsToChangeSiteVisibility" property to "false" and assigning a security group to "Manage Site Visibility" in Power Platform Admin Center. If this is used, consider requiring PIM elevation for that group.	MS: Site Visibility in Power Platform SOGP AC1.4.1
11.17	Authentication can use OpenIDConnect, SAML 2.0/WS-Fed, or OAuth 2.0. Microsoft make configuration guides available for several 3rd party identity providers including Entra ID, Azure B2C, ADFS, LinkedIn, X and Local Authentication. NOTE: Local Authentication is not recommended.	MS: Overview of authentication in Power Pages
11.18	Power Pages supports open registration, which is least restrictive and allows users to sign themselves up. Consider if this is suitable for your site before configuring.	MS: Overview of authentication in Power Pages
11.19	The anonymous role is intended only for table permissions - it doesn't respect other rules or permissions.	MS: Create & assign webroles
11.20	Use column permissions to further restrict data than is possible with table permissions.	MS: Set Column Permissions
11.21	Column permissions can (currently) only be used with the Power Pages Portal Web API.	MS: Set Column Permissions

Reference	Minimum requirement	Control reference
11.22	Note that column permissions are applied after table permissions, so if no table permissions for the user, the column permissions will not be evaluated.	MS: Set Column Permissions
11.23	If table permissions grant access, and if no column permissions exist, all columns are accessible.	MS: Set Column Permissions
11.24	Pages have permissions. They can have their own or inherit them.	MS: Set Page Permissions
11.25	The "Grant Change" permission takes precedence over "Restrict Read".	MS: Set Page Permissions
11.26	Power Pages is a HTTPS only platform. If using a custom domain, you need to bring your own TLS certificate.	MS: Power Pages Security Whitepaper
11.27	Consider cookie security and whether the "SameSite" attribute should be set to "Strict".	MS: Power Pages Security Whitepaper Use Service Admin roles to manage your tenant
11.28	Limit Power Pages creation to admin users.	CISA Power Platform Secure Cloud Business Applications: 7.1.1
12.	**Environments**	
12.1	Limit environment creation to admins, including trials.	IAM & PS Blueprints, volume 4, section 6.4.4 CIS Microsoft Dynamics 365 Power Platform: 2.1 CISA Power Platform Secure Cloud Business Applications: 3.1.1 CISA Power Platform Secure Cloud Business Applications: 3.1.2
12.2	Use UK environments only.	IAM & PS Blueprints, volume 4, section 6.4.5 CIS Microsoft Dynamics 365 Power Platform: 2.4

Reference	Minimum requirement	Control reference
12.3	In managed environments, there are 3 options for limiting how an app is shared which may be useful depending on the use case: not set (open sharing), exclude set security groups, "limit total" (set a limit on the number of people it can be shared with).	MS: Power Platform Limit Sharing
12.4	Use environment groups to set policies at a high level, which are then inherited by each environment below.	MS: Increase efficiency with Power Platform Governance Features MS: Develop a tenant strategy to adopt PP at scale
12.5	Users with delegated administrative permissions on environments cannot change items set by policies at the group level.	MS: Increase efficiency with Power Platform Governance Features
12.6	Use tenant isolation, either inbound, outbound, or in both directions, to control external connections. Note, this control only works for connectors using Entra ID based authentication in Canvas apps and Flows.	Microsoft Internal Security Best Practices: Secure Power Platform Development Develop a tenant strategy to adopt PP at scale CISA Power Platform Secure Cloud Business Applications: 5.1.1 CISA Power Platform Secure Cloud Business Applications: 5.1.2 MS: Cross tenant inbound and outbound restrictions
12.7	Data sharing agreements should be in place for any exported data.	SOGP IM1.5.1
12.8	IP based allow lists are available but requires a premium licensing, on top of E5. Currently this is IPv4 only.	MS: IP firewall in Power Platform environments

Reference	Minimum requirement	Control reference
12.9	Note that every employee has access to the Default Environment - therefore it needs to be secured.	MS: Secure the default environment
12.10	It is recommended to rename the default environment to something like "Personal Productivity Environment" to signal the intent that it is not for production apps intended for wide adoption.	MS: Secure the default environment
12.11	It is recommended to use custom roles for each environment so environment admin rights can be delegated, without needing to use the highly privileged Power Platform Admin role.	MS: Secure the default environment
12.12	Make use of the Power Platform hub - a SharePoint site template that will allow you to easily showcase use-cases, your rules/policy/guidance on usages, building guides, and support contacts.	MS: Secure the default environment SOGP ST1.2.3 SOGP ST1.2.4
12.13	Consider default environment routing to ease management and minimise encroachment.	MS: Develop a tenant strategy to adopt PP at scale
12.14	Consider automating the clear up of old/unused environments.	MS: Develop a tenant strategy to adopt PP at scale SOGP SD4.4.1
12.15	Securely decommission old environments, including revoking credentials.	SOGP UA2.1.12
12.16	For larger apps, consider using a development methodology and embed secure development practices.	SOGP SD1.1.3 SOGP SD1.2.2 SOGP SD3.1.2
12.17	Use a series of environments and promote dev to test to production.	SOGP SD1.3.1
12.18	Use isolated environments to control the blast radius of issues.	SOGP SD1.3.2

Reference	Minimum requirement	Control reference
12.19	Conduct quality checks before promoting apps to production.	SOGP SD1.5.1 SOGP SD3.2.1
12.20	Set acceptance criteria before promoting to production.	SOGP SD4.1.1
12.21	Conduct post-implementation reviews and learn from them.	SOGP SD4.3.1
13.	**Group management**	
13.1	Use security groups to control application access.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 1 SOGP UA2.2.8 SOGP TI1.1.2 SOGP TI1.1.8
13.2	Use security groups to control Dataverse access.	CIS Microsoft Dynamics 365 Power Platform: 1.1
13.3	Remember the "everyone" group includes guests.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 5
13.4	Regularly review group membership for privileged roles.	CIS Microsoft Dynamics 365 Power Platform: 4.1
14	**Dataverse**	
14.1	For role-based security, associate roles with users, with Dataverse teams, or with Dataverse business units, as required.	MS: Security concepts in Dataverse
14.2	Dataverse business units are classed as security boundary. While they can be structure them to map an organisational structure, it is recommended to order them to align to security requirements.	MS: Security concepts in Dataverse
14.3	Dataverse business units should be mapped 1:1 to an Entra ID security group for easier rights management.	MS: Security concepts in Dataverse

Reference	Minimum requirement	Control reference
14.4	Dataverse business units can be further split into Teams - Owning teams and Access teams. Owning teams can own (write) records, Access teams can read records.	MS: Security concepts in Dataverse
14.5	Use conditional access policies for Dataverse.	MS: Security concepts in Dataverse
14.6	Apply RBAC to Dataverse.	Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 2 Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks: 4
14.7	Note that Dataverse and Dataverse for Teams are different products with different capabilities. The latter is a targeted set of features at a lower cost, but with increased environment limits, fewer integrations and fewer security features (i.e. no auditing, record sharing, or field-level security). Use of Dataverse for Teams should be a conscious decision, taken after a full evaluation of the needs of the use-case and taken in conjunction with local Information Assurance processes.	MS: How are Dataverse for Teams and Dataverse different?

Suggested security review questions

From: Microsoft Internal Security Best Practices: Secure Power Platform Development

Question	Notes
Does it use 3rd party connectors?	Is data leaving the tenant?
Are there any custom connectors?	Is the authentication robust?
Is an object being shared?	If so, what level of sharing is being used?
Is it accessible by external users (B2B or B2C)?	Are NDA's in place?
Any HTTP connectors?	They can bypass tenant boundaries so use endpoint filtering
Is data being explicitly exported?	Is the source "public" data only? Is the destination appropriate?
Is the app being over shared?	Who can use it?
How many co-owners does it have?	Remember they can re-use connectors, including authentication
Is it a "personal productivity" app or a "production" app?	Personal probably has fewer than 50 users and 500 sessions per month
Is the DLP policy overly broad?	Check least privilege is being followed
For database activities (CRUD), are stored procedures being used?	Is user input used in an un-sanitised way?

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.

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

Forces adopting this guidance who have no existing Power Platform implementation should be able to adopt this as-is. Those forces who have existing Power Platform environments should start with a gap analysis and come up with a remediation plan to accept or remediate any gaps.

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	30/08/24
1.0	PDS Cyber	Updated to inc. NCPSWG comments.	02/10/24

Approvals

Version	Name	Role	Date
1.0	NCPSWG	National Cyber Policy & Standards Working Group	02/10/24

Document References

Document Name	Version	Date
ISF Standard of Good Practice	2024	28/03/2024
NIST SP800-218 Secure Software Development Framework	1.1	Feb-22
CISA Power Platform Secure Cloud Business Applications	1	Dec-23
CIS Microsoft Dynamics 365 Power Platform	1.0.0	20/12/2022
Power Platform security FAQs (link)	Web page	11/04/2024
Content security policy (link)	Web page	14/06/2024
Use Microsoft SQL Server securely with Power Apps (link)	Web page	07/05/2024
OWASP Low-Code/No-Code Top 10 (link)	Web page	02/07/2023
Power Pages security (link)	Web page	12/05/2024
Security issues (preview) (link)	Web page	12/02/2024
Configure site settings for websites (link)	Web page	09/07/2024
Configure Web Application Firewall for Power Pages (link)	Web page	23/08/2023
Content Delivery Network (link)	Web page	12/08/2024
Run security scan (preview) (link)	Web page	31/05/2024
Site visibility in Power Pages (link)	Web page	25/07/2024
Overview of authentication in Power Pages (link)	Web page	03/11/2023
Create and assign web roles (link)	Web page	06/11/2023
Portals Web API overview (link)	Web page	15/09/2023
Assign table permissions (link)	Web page	25/07/2024

Document Name	Version	Date
Set column permissions (link)	Web page	08/07/2023
Configuring table permissions (link)	Web page	25/07/2024
Set page permissions (link)	Web page	05/03/2024
Power Pages security white paper (link)	Web page	31/08/2023
Microsoft Power Platform Mitigation for the OWASP Low Code/No Code Top 10 Security Risks (link)	Web page	11/04/2024
Limit sharing (link)	Web page	08/02/2024
Preview Microsoft Power Platform environment groups and rules (link)	Web page	04/04/2024
Microsoft Internal Security Best Practices: Secure Power Platform Development (link)	Web page	17/09/2021
Security concepts in Microsoft Dataverse (link)	Web page	23/07/2024
Use service admin roles to manage your tenant (link)	Web page	24/07/2024
Cross-tenant inbound and outbound restrictions (link)	Web page	26/04/2024
IP firewall in Power Platform environments (link)	Web page	27/06/2024
Safeguarding Dataverse sessions with IP cookie binding (link)	Web page	27/06/2024
Secure the default environment (link)	Web page	17/05/2024
View Power Platform administrative logs using auditing solutions in Microsoft Purview (link)	Web page	23/07/2024
Power Platform licensing FAQs (link)	Web page	04/03/2024
Power Automate licensing FAQ (link)	Web page	10/07/2024
Develop a tenant environment strategy to adopt Power Platform at scale (link)	Web page	13/06/2024

Document Name	Version	Date
Set the preferred solution (link)	Web page	03/07/2024
Overview of pipelines in Power Platform (link)	Web page	06/05/2024
Microsoft Enterprise Security with Microsoft Power Platform (link)	Web page	26/02/2024
How are Dataverse for Teams and Dataverse different? (link)	Web page	16/12/2022