|  |  |  |
| --- | --- | --- |
|  |  |  |
| Security Design & Review Guidelines **Version 1.0**  ISV Solutions & SI Capability Enablement - **Business Applications** |
|  |
| **Partner:** TBD  **Key partner contact(s) e-mail(s) and role(s):** TBD **Solution AppSource Name:** TBD **Date:** TBD |

**Your privacy is important to us. Please do not include any personal or sensitive information. To learn more read** [**Microsoft Privacy Statement**](https://privacy.microsoft.com/en-US/privacystatement)

**Table of Contents**

[Security Design & Review Process 1](#_Toc43721089)

[1. Security Design Life Cycle 2](#_Toc922982197)

[2. Business Applications Security Recap 4](#_Toc1053841202)

[3. Secure by Design 4](#_Toc1269577436)

[4. Secure by Default 7](#_Toc789827951)

[5. Secure Operations 12](#_Toc1582941)

[Appendix: 15](#_Toc813725022)

# **Security Design & Review Process**

The purpose of this document is to provide comprehensive best practices, enablement topics and a thorough review of partner solutions for Dynamics 365 and Power Platform, specifically tailored for the Secure Future Initiative. This document is designed to guide solution architects in implementing robust security measures across various stages of solution development and deployment and product implementation.

The document is structured into three main sections: Secure by Design, Secure by Default, and Secure in Operations. Each section offers topics, and best practices to ensure the security of solutions built on Dynamics 365, Power Platform, and Copilot studio.

**Secure by Design:** This section focuses on the principles and practices that should be incorporated during the initial design phase of the solution. It includes guidelines on threat modeling, secure design practices, and design reviews to identify and mitigate potential security risks early in the development process.

**Secure by Default:** This section emphasizes the importance of configuring systems and applications securely out of the box. It covers best practices for default settings, access controls, and configuration management to ensure that the deployed solutions are secure from the outset.

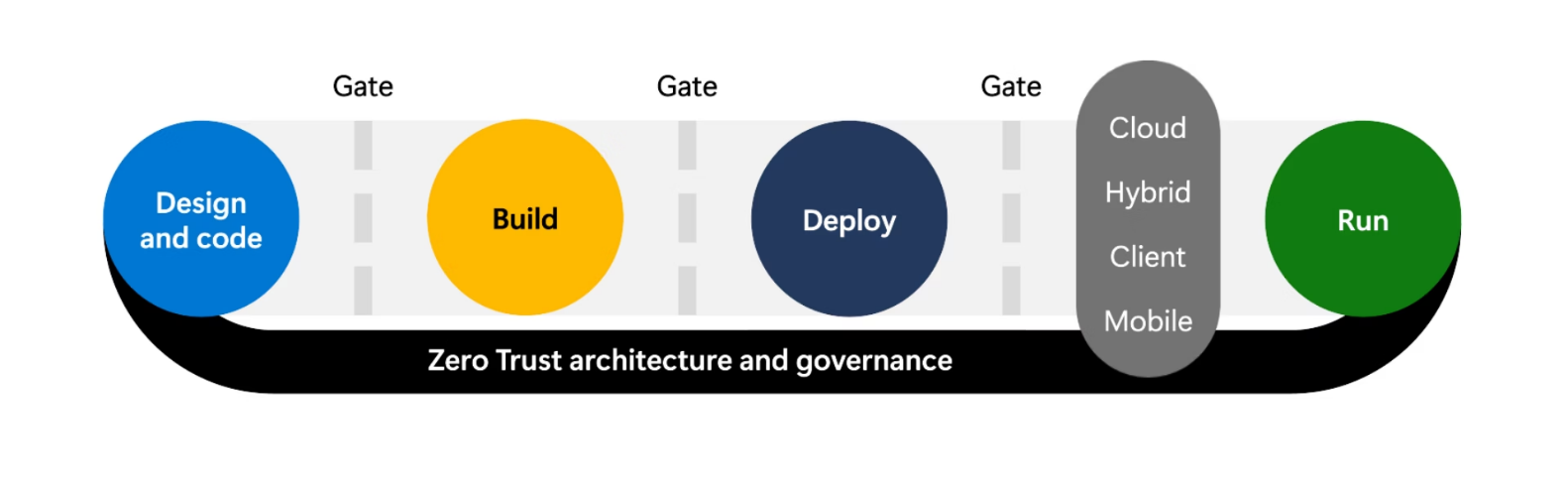
**Secure Operations:** This section provides best practices for maintaining and monitoring the security of solutions during their operational lifecycle. It includes topics on incident response, continuous monitoring, and regular security assessments to ensure ongoing protection against emerging threats.

By following the guidelines and best practices outlined in this document, solution architects can ensure that their solutions are secure, resilient, and compliant with industry standards and regulations. This document serves as a valuable resource for architects to build and maintain secure solutions that meet the high standards of the Secure Future Initiative.

Partner can review more about [Security above all else – expanding Microsoft’s Secure Future Initiative.](https://www.microsoft.com/en-us/security/blog/2024/05/03/security-above-all-else-expanding-microsofts-secure-future-initiative)

1. **Security Design Life Cycle**

The Security Development Lifecycle (SDL) is the approach Microsoft uses to integrate security into DevOps processes (sometimes called a DevSecOps approach). You can use the [SDL guidance and documentation](https://www.microsoft.com/en-us/securityengineering/sdl/) to adapt this approach and practices to your organization.

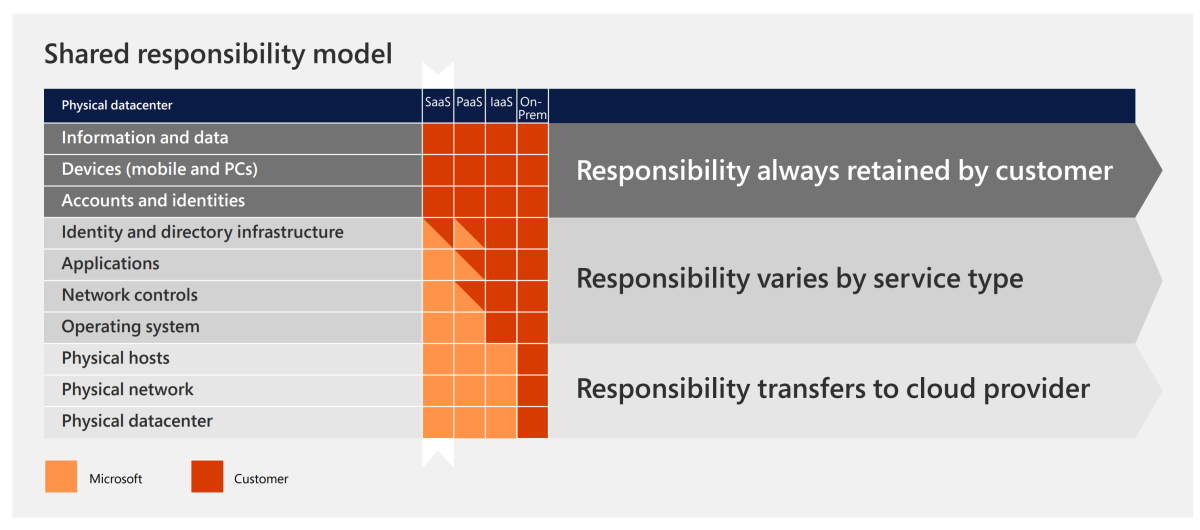


Security risks (and the need to mitigate them) can occur at any point in the development lifecycle:

* **Design** – ensure that the design doesn’t naturally allow attackers to easily gain unauthorized access to the workload, its data, or other business assets in the organization.
* **Code** – ensure that writing (and re-use) of code doesn’t allow attackers to easily take control of the application to perform unauthorized actions that harm customers, employees, systems, data, or other business assets. Developers should also work in a secure environment that doesn’t allow attackers to do this without their knowledge.
* **Build and Deploy** – ensure that the continuous integration and continuous deployment (CI/CD) processes don’t allow unauthorized users to alter the code and allow attackers to compromise it.
* **Run** – ensure that environment running the code (cloud, servers, mobile devices, others) follows security best practices across people, process, and technology to avoid attackers compromising and abusing the workload. This includes the adoption of well-established best practices, security baseline configurations, and more.
* **Zero Trust architecture and governance** – All of these stages should follow Zero Trust principles to assume breach (assume compromise), explicitly verify trust, and grant the least privilege required for each user account, machine/service identity, and application component.

|  |
| --- |
| **SDL Practices** |
| [1. Establish security standards, metrics, and governance](https://aka.ms/sdl/practices/security-program-management) |
| [2. Require use of proven security features, languages, and frameworks](https://aka.ms/sdl/practices/secure-platforms) |
| [3. Perform security design review and threat modeling](https://aka.ms/sdl/practices/secure-by-design) |
| [4. Define and use cryptography standards](https://aka.ms/sdl/practices/cryptography) |
| [5. Secure the software supply chain](https://www.microsoft.com/securityengineering/sdl/practices/sscs) |
| [6. Secure the engineering environment](https://www.microsoft.com/securityengineering/sdl/practices/secure-dev-infra) |
| [7. Perform security testing](https://aka.ms/sdl/practices/security-testing) |
| [8. Ensure operational platform security](https://aka.ms/sdl/practices/operational-security) |
| [9. Implement security monitoring and response](https://aka.ms/sdl/practices/monitoring-and-response) |
| [10. Provide security training](https://aka.ms/sdl/practices/security-training)   1. **Business Applications Security Recap** |

A few topics below to set some ground rules on Security landscape for business applications as follows. If you are new to the topic, it is highly advised to go through recap topics before proceeding to the next sections.



* + [Security Strategy](https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/security)
  + [Security controls](https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/security-strategy-security-controls)
  + [Security in the customer engagement apps](https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/security-strategy-product-ce)
  + [Security in Power Pages](https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/security-strategy-product-portals)
  + [Security in finance and operations apps](https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/security-strategy-product-oa)
  + [Day one priorities](https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/security-strategy-day-one-priority)
  + [Checklist](https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/security-strategy-checklist)

1. **Secure by Design**

**Objective:** To ensure that security is integrated into the design phase of solutions built on Dynamics 365, Power Platform, and Copilot Studio.

**Key Topics:**

* Security architecture principles
* Threat modeling and risk assessment
* Secure design practices

**Best Practices:**

* Incorporate security requirements early in the design process
* Use secure design patterns and frameworks

**Review Components:**

|  |  |  |
| --- | --- | --- |
| Topic | Additional Resources | Evaluation & Recommendations |
| Copilot Scenarios   * Are scenarios aligned with [Responsible AI guidelines & FAQs](https://learn.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/responsible-ai/responsible-ai-overview). * Are [data loss prevention policies for copilots configured](https://learn.microsoft.com/en-us/microsoft-copilot-studio/admin-data-loss-prevention). * [Has Security FAQs for Copilot Studio reviewed?](https://learn.microsoft.com/en-us/microsoft-copilot-studio/security-faq) | * [Responsible AI FAQs for Copilot Studio](https://learn.microsoft.com/en-us/microsoft-copilot-studio/responsible-ai-overview) * **F&O:** [Chat with finance and operations data on Microsoft 365 Copilot](https://learn.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/m365-copilot/chat-with-fno-data-on-m365copilot) * **F&O:** [Architecture of Copilot in finance and operations apps](https://learn.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/copilot/copilot-architecture) |  |
| Regulatory & Data Location requirements:   * What are the regulatory requirements and norms you need to comply with? * Do you have hard requirements as to where the data must be located? * Validate solution and implementation comply with [regulatory requirements](https://www.microsoft.com/en-us/trust-center/product-overview) for data security. * Understand solutions’ [data location](https://www.microsoft.com/en-us/trust-center/privacy/data-location) impact on regulatory requirements. | Microsoft Data Protection resources.   * [Security and geographic data residency in Copilot Studio](https://learn.microsoft.com/en-us/microsoft-copilot-studio/geo-data-residency-security) * **F&O:** [Regulatory Configuration Services (RCS) Globalization features](https://learn.microsoft.com/en-us/dynamics365/finance/localizations/global/rcs-globalization-feature) |  |
| Securing Data Model & Integrations  Is data model designed keeping [secured design principals](https://www.microsoft.com/en-us/securityengineering/sdl/) aligned?   * Familiarize with [Security concepts in Microsoft Dataverse](https://learn.microsoft.com/en-us/power-platform/admin/wp-security-cds) * [Security Workshop topics](https://learn.microsoft.com/en-us/training/modules/fast-track-security/2-security-workshop-topics) (Implementation / Solutioning) | * [Security concepts for developers](https://learn.microsoft.com/en-us/power-apps/developer/data-platform/security-concepts) * [Review security model for Dynamics 365 solutions](https://learn.microsoft.com/en-us/training/modules/fast-track-security/) * [Security in Microsoft Dataverse](https://learn.microsoft.com/en-us/power-platform/admin/wp-security) * **BC:** [Layered security model in Business Central](https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/security/security-application) * **F&O:** [Securing data entities](https://learn.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/data-entities/security-data-entities) * **F&O:** [Integrate your Dynamics 365 apps with other solutions](https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/integrate-other-solutions) |  |
| Copilot Studio   * Is Copilot Studio components reviewed for security? * Do you need to enforce web and Direct Line channel security? * Is the copilot working unauthenticated, authenticated, or both? * Do you plan to use DLP policies to enforce Copilot Studio allowed channels and authentication settings?   [Manage Microsoft Copilot Studio](https://learn.microsoft.com/en-us/training/modules/implement-power-virtual-agents/) | * Review Bot topic permissions * Review Bot entities and flow permissions * Review administrator, export, import permissions * Enable Monitoring * Authentication |  |
| Environment Strategy  Evaluate and choose the right environment strategy.   * [Single vs. Multi-tenant strategy](https://learn.microsoft.com/en-us/power-platform/admin/multiple-online-environments-tenants) | * [Control user access to environments: security groups and licenses](https://learn.microsoft.com/en-us/power-platform/admin/control-user-access) * **F&O:** [Plan your environment strategy for Dynamics 365](https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/environment-strategy-overview) |  |

1. **Secure by Default**

**Objective:** To ensure that solutions are configured securely out of the box, minimizing the need for extensive post-deployment security configurations.

**Key Topics:**

* Default security settings and configurations
* Access control and identity management
* Data protection and encryption

**Best Practices:**

* Enable multi-factor authentication (MFA) by default
* Apply least privilege access principles
* Use built-in encryption features for data at rest and in transit

|  |  |  |
| --- | --- | --- |
| Topic | Additional Resources | Evaluation & Recommendations |
| Identity Management   * Do you enforce strong requirements for authentication? * How do you control privileged users access to sensitive data? * Make sure [strong MFA authentication](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks) is implemented. * How do you manage secrets? Store and manage secrets, keys, certificates in [Key Vault](https://learn.microsoft.com/en-us/azure/key-vault/general/) * Do you use service principals or managed identities? * Use [Azure Managed Identities](https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/) for Integrations, Data Exchange and Plugins. | * [Use managed identities for Dataverse plug-ins](https://learn.microsoft.com/en-us/power-platform/release-plan/2024wave1/power-platform-governance-administration/use-managed-identities-dataverse-plug-ins) * [Use managed identities for Azure with your Azure data lake storage](https://learn.microsoft.com/en-us/power-apps/maker/data-platform/azure-synapse-link-msi) * **BC:** Using App Key Vaults with Business Central Extensions * **F&O:** [Setup Azure Key Vault client](https://learn.microsoft.com/en-us/dynamics365/finance/localizations/global/setting-up-azure-key-vault-client) |  |
| Role based Security  All user roles must be on least privilege principle.  [Get started with security roles in Dataverse](https://learn.microsoft.com/en-us/training/modules/get-started-security-roles/?wt.mc_id=cybersecurityawarenessmonth2022_csaalignedpost_blog_wwl) | * [Leverage security role templates](https://learn.microsoft.com/en-us/power-apps/developer/data-platform/security-roles) * **F&O:** [Role based security](https://learn.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/sysadmin/role-based-security) * **F&O:** [Active Directory security groups](https://learn.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/sysadmin/active-directory-security-group) * **F&O:** [Extensible data security policies](https://learn.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/sysadmin/extensible-data-security-policies) |  |
| Review privileged accounts security strategy   * Understand privileged roles for Microsoft 365, Dynamics 365 and Power Platform * Consider Just-In-Time access approach to grant limited elevated privileges * Leverage Service principals and Entra Applications for integrations & deployments | * [Configure user security in an environment](https://learn.microsoft.com/en-us/power-platform/admin/database-security) * [Use service admin roles to manage your tenant](https://learn.microsoft.com/en-us/power-platform/admin/use-service-admin-role-manage-tenant) * [Create an administrative user and prevent elevation of security role privilege](https://learn.microsoft.com/en-us/power-platform/admin/prevent-elevation-security-role-privilege) * [Enable just-in-time database access](https://learn.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/database/database-just-in-time-jit-access) * [Manage application users in the Power Platform admin center](https://learn.microsoft.com/en-us/power-platform/admin/manage-application-users) * [Register a Microsoft Entra app and create a service principal](https://learn.microsoft.com/en-us/entra/identity-platform/howto-create-service-principal-portal) * [Leverage security role templates](https://learn.microsoft.com/en-us/power-apps/developer/data-platform/security-roles) |  |
| Data Loss Policies Control   * How do you ensure that internal confidential data doesn’t get available externally? * Do you plan to use DLP policies to enforce allowed or blocked Power Automate connectors or HTTP requests? * [Evaluate and provision DLP controls](https://learn.microsoft.com/en-us/power-platform/admin/wp-data-loss-prevention) | * [Cross-tenant inbound and outbound restrictions](https://learn.microsoft.com/en-us/power-platform/admin/cross-tenant-restrictions) * [Email exfiltration controls for connectors](https://learn.microsoft.com/en-us/power-platform/admin/block-forwarded-email-from-power-automate) |  |
| Audit & Logging   * Do you audit and review access periodically? * Do you plan to use the Center of Excellence Starter Kit to monitor your copilots in your tenant? * Do you have other technical monitoring requirements and plans? * [Manage Dataverse auditing](https://learn.microsoft.com/en-us/power-platform/admin/enable-use-comprehensive-auditing) * [Evaluate and enable Entra Audit logs](https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-audit-logs) * [Monitor Dataverse usage](https://learn.microsoft.com/en-us/power-platform/guidance/adoption/cds-usage) | * [Microsoft Dataverse and model-driven apps activity logging](https://learn.microsoft.com/en-us/power-platform/admin/enable-use-comprehensive-auditing) |  |
| Application Telemetry   * How do you plan to technically monitor your integrations and cloud flows? * [Azure Application Insights](https://learn.microsoft.com/en-us/power-platform/admin/overview-integration-application-insights) | * [Center of Excellence Starter kit](https://learn.microsoft.com/en-us/power-platform/guidance/coe/starter-kit) |  |
| Encryption   * [Manage the encryption key for environment](https://learn.microsoft.com/en-us/power-platform/admin/manage-encryption-key) * [Setup Lockbox (if applicable)](https://learn.microsoft.com/en-us/power-platform/admin/about-lockbox) | * **BC:** [Encrypting Data in Dynamics 365 Business Central](https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/developer/devenv-encrypting-data) * **F&O:** [Encryption in finance and operations apps](https://learn.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/sysadmin/encryption) * **F&O:** [Customer managed keys for encryption at rest](https://learn.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/sysadmin/customer-managed-keys) |  |
| Network Controls   * Do you have network security requirements? * [Evaluate Service tags](https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview) | * [Use Azure ExpressRoute with Microsoft Power Platform](https://learn.microsoft.com/en-us/power-platform/guidance/expressroute/overview) * [Virtual Network support for Power Platform overview](https://learn.microsoft.com/en-us/power-platform/admin/vnet-support-overview) * [Export APIs from Azure API Management to the Power Platform](https://learn.microsoft.com/en-us/azure/api-management/export-api-power-platform) * **BC:** [Use Azure security service tags to restrict network access from/to Business Central](https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/security/security-service-tags) |  |
| Data management strategy (Reporting / outside sources)   * [Row-level security (RLS) with Power BI](https://learn.microsoft.com/en-us/fabric/security/service-admin-row-level-security) | * [Evaluate & Review DirectQuery / SQL Query with PowerBI (if applicable)](https://learn.microsoft.com/en-us/power-query/connectors/dataverse) |  |
| Security Best Practices | * [Safeguarding Dataverse sessions with IP cookie binding](https://learn.microsoft.com/en-us/power-platform/admin/block-cookie-replay-attack) * [Configure IP firewall in Power Platform environments](https://learn.microsoft.com/en-us/power-platform/admin/ip-firewall) * [Restrict Guest user permissions](https://learn.microsoft.com/en-us/power-platform/admin/control-user-access) * [Enable tracking user access for continuous improvements](https://learn.microsoft.com/en-us/power-platform/guidance/adoption/access-usage)   **F&O:** [RSAT User-based authentication](https://learn.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/perf-test/rsat/rsat-user-based-authentication) |  |

1. **Secure Operations**

**Objective:** To maintain and enhance the security of solutions during their operational lifecycle.

**Key Topics:**

* Continuous monitoring and incident response
* Patch management and vulnerability assessments
* Security training and awareness

**Best Practices:**

* Implement continuous security monitoring and logging
* Regularly update and patch systems
* Conduct periodic security training for all stakeholders

|  |  |  |
| --- | --- | --- |
| Topic | Additional Resources | Evaluation & Recommendations |
| Data archival & retention | * **F&O:** [Archive data in Dynamics 365 finance and operations apps with Dataverse](https://learn.microsoft.com/en-us/dynamics365/fin-ops-core/dev-itpro/sysadmin/archive-data) * **Purview** * [View Copilot Studio audit logs](https://learn.microsoft.com/en-us/microsoft-copilot-studio/admin-logging-copilot-studio) * [View the Power Platform connector activity logs](https://learn.microsoft.com/en-us/power-platform/admin/connector-events-power-platform) * **BC:** [Auditing in Purview](https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/auditing/audit-events-in-purview) |  |
| Environment Strategy   * Are you doing periodic security assessments? | * [Stay current with Dynamics 365 service updates](https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/service-solution-service-updates) * [Security assessment for your tenant](https://learn.microsoft.com/en-us/power-platform/admin/security/security-posture-overview) * **F&O:** [Request credentials to access D365 finance and operations product database](https://learn.microsoft.com/en-us/power-platform/developer/unified-experience/finance-operations-product-db-access) |  |
| Monitor Telemetry Analytics   * Do you have specific governance requirements? * Evaluate Security Information and Event Management (SIEM) implementation * Evaluate Security Orchestration, Automation, and Response (SOAR) implementation * Evaluate Data Governance strategy and solution implementation | * [Dynamics 365 connector for Microsoft Sentinel](https://learn.microsoft.com/en-us/azure/sentinel/data-connectors/dynamics-365) * [Data governance via Azure Purview](https://learn.microsoft.com/en-us/purview/register-scan-dataverse?tabs=MI) * [Power Apps Tenant-wide analytics](https://learn.microsoft.com/en-us/power-platform/admin/tenant-level-analytics) * [Power Automate analytics](https://learn.microsoft.com/en-us/power-platform/admin/analytics-flow) * [Using Data Lake](https://learn.microsoft.com/en-us/power-platform/admin/self-service-analytics) * [Deploy the Microsoft Sentinel solution for Microsoft Power Platform](https://learn.microsoft.com/en-us/azure/sentinel/business-applications/deploy-power-platform-solution) * **F&O:** [Microsoft Sentinel solution for Dynamics 365 Finance and Operations](https://learn.microsoft.com/en-us/azure/sentinel/dynamics-365/dynamics-365-finance-operations-solution-overview) |  |
| Security Best Practices | * Apply [Context based AD policies](https://learn.microsoft.com/en-us/power-platform/guidance/adoption/conditional-access) * [Block access by location with Microsoft Entra Conditional Access](https://learn.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules) * [Continuous access evaluation](https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-continuous-access-evaluation) * [Services Trust Portal Guidance](https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3) * [Penetration Testing Rules of Engagement](https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement?rtc=1) |  |

Further guidelines listed in this artifact are not exhausted, implementers are always advised to look at product updates for updated guidance.

**Appendix:**

* [Dynamics 365 FastTrack Architecture Insights](https://learn.microsoft.com/en-us/shows/dynamics-365-fasttrack-architecture-insights/best-practices-power-platform-and-dataverse-security)
* [Microsoft Power Platform and Dataverse: Skill up on security by design](https://techcommunity.microsoft.com/t5/microsoft-learn-blog/microsoft-power-platform-and-dataverse-skill-up-on-security-by/ba-p/3250818)
* [Cybersecurity Awareness - Power Platform](https://learn.microsoft.com/en-us/collections/g1kbpkdg628q7?wt.mc_id=cybersecurityawarenessmonth2022_csaalignedpost_blog_wwl)
* [Protecting Data with Dataverse Part 2: Security from Internal Threats (Users)](https://www.microsoft.com/en-us/power-platform/blog/power-apps/protecting-data-with-dataverse-part-2-security-from-internal-threats-users/?msockid=1de4bf3d1c9d60712ccbabaa1dde61a6)
* [Embrace proactive security with Zero Trust](https://www.microsoft.com/en-us/security/business/zero-trust)
* [Power Platform and Dynamics 365 Apps – Guide to security and Compliance](https://aka.ms/D365SecurityAndComplianceGuide)
* [Dynamics 365 implementation guidance](https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/overview#p=192)
* [Solution architect series: Model security for Power Platform solutions](https://learn.microsoft.com/en-us/training/modules/model-security/?wt.mc_id=cybersecurityawarenessmonth2022_csaalignedpost_blog_wwl)
* [Implementation recommendations for Microsoft Power Platform environments](https://learn.microsoft.com/en-us/training/modules/implementation-recommendations/)
* [Power Platform security FAQs](https://learn.microsoft.com/en-us/power-platform/admin/security/faqs)
* [Secure your Dynamics 365 data and apps](https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/security)
* [Microsoft Power Platform security and governance documentation](https://learn.microsoft.com/en-us/power-platform/admin/security)
* [IT Governance Controls for Your Copilot agents](https://www.microsoft.com/en-us/power-platform/blog/power-apps/it-governance-controls-for-your-copilot-agents/)