<https://github.com/Azure/fta-deliveryhowto/blob/master/articles/security/data-security-checklist.md#corefundamental>

***Data Security Checklist and Best Practices***

|  |  |
| --- | --- |
| Item | Links |
| Enable Azure Security Center. After enabling Security Centre, Review any detected items for any issues which require immediate action. | [QuickStart: Setting up Azure Security center](https://docs.microsoft.com/en-us/azure/security-center/security-center-get-started) |
| If you do not have any other SIEM product, Enable Azure Sentinel to support security investigation exercises | [What is Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/overview)  [QuickStart: Onboard Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard) |
| Create a *Data Breach Response Plan*. A plan will provide the team a roadmap to follow when a breach is discovered. Under GDPR, there are significant compliance requirements in the case of a data breach. | [Do you have a data breach response plan?](https://www.itgovernance.co.uk/blog/do-you-have-a-data-breach-response-plan)  [Building your own security incident response process](https://msrc-blog.microsoft.com/2019/07/01/inside-the-msrc-building-your-own-security-incident-response-process/) |
| Review the Azure Architecture Centre, specifically the Security pillar. There is a wealth of information here to Design, Monitor and Optimize your overall Cloud Security position | [Azure Architecture Centre - Security pillar](https://docs.microsoft.com/en-us/azure/architecture/framework/security/overview) |
| DO NOT store usernames, passwords, keys, connection strings, or any other secrets in scripts, code, or repositories. |  |
| Use Azure Key Vault to secure credentials, connection strings, and secrets. |  |
| Review Azure Defender and understand the offerings available for different Azure Services | [Introduction to Azure Defender](https://docs.microsoft.com/en-us/azure/security-center/azure-defender) |
| Configure email notifications for Security Centre Alerts to help reduce the time-to-response and time-to-resolution for any detected alerts. | [Configure email notifications for Alerts](https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details) |
| *Prepare for battle.* On a daily basis, review all Alerts raised in Security Center for the Data-tier, correlate with applicable logs from [Application Insights](https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview), detect unusual access patterns, and take action as appropriate.  **Note:** There are a range of responses from notifying your security team (Security Operations Center) to locking down/shut down the resources. Your response should be based on your organizations Security Incident Response Plan. | [Tutorial: Triage, investigate and respond to Security Alerts](https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-incident)  [Manage security incidents in Azure Security Centre](https://docs.microsoft.com/en-us/azure/security-center/security-center-incident)  MS Security Incident Response Guides [v1](https://docs.microsoft.com/en-us/azure/security/benchmarks/security-control-incident-response) and [v2](https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-incident-response)  - v1: [Building your own security incident response process](https://msrc-blog.microsoft.com/2019/07/01/inside-the-msrc-building-your-own-security-incident-response-process/)  - v2: [Incident Response reference guide](https://docs.microsoft.com/en-us/microsoft-365/downloads/IR-Reference-Guide.pdf) |
| Centralize the collection of audit data for reporting and visualization. We recommend sending the data to Log Analytics. For customers who are not comfortable with a service in *Preview*, the data can be stored in blob storage. | [Security Fundamentals: Azure Security logging and auditing](https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit) |
| Practice executing your *Data Breach Response Plan* periodically, by running smoke-tests with the Security team as well as any other involved teams. |  |
| Follow the Principle of Least Privilege when implementing security permissions/controls. Only give users and app roles the minimum permissions they need to perform the required function/operation. | - [SQL DB](https://docs.microsoft.com/en-us/azure/azure-sql/database/security-best-practice#implement-principle-of-least-privilege)  - [ADO.NET](https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/security-overview#the-principle-of-least-privilege) |
| *Trust but verify.* Encourage developers to focus on security and adopt secure development practices. Perform penetration testing and review Security Center findings. | [Penetration Tests and Red Team Exercises](https://docs.microsoft.com/en-us/azure/azure-sql/database/security-baseline#penetration-tests-and-red-team-exercises) |
| Perform Threat Modelling. Identify the specific security risks and threats that are most relevant for the data environment. Determine the most important events and metrics to measure to ensure you are collecting data that will be meaningful in identifying these risks. | [Microsoft Security Development Lifecycle - Threat Modeling](https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling)  [Microsoft Threat Modelling Tool overview](https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-feature-overview)  [Getting started with the Threat Modelling Tool](https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started) |
| Review the [Azure Security Fundamentals](https://docs.microsoft.com/en-us/azure/security/fundamentals/), specifically the [Data Security, encryption and storage](https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview) section. |  |
| Review the [Azure SQL Security Playbook](https://docs.microsoft.com/en-us/azure/azure-sql/database/security-overview). It provides an overview of the multi-layered approach for defense in depth of the data platform. Consider how the Zero Trust security model may help to further secure the data platform. | [Azure SQL Security Playbook](https://docs.microsoft.com/en-us/azure/azure-sql/database/security-overview)  [Defense in depth security in Azure](https://azure.microsoft.com/en-us/resources/videos/defense-in-depth-security-in-azure/)  [Zero Trust Security](https://www.microsoft.com/en-us/security/business/zero-trust) |