O365 Information Security standard

**AFG-EIT-IS-SD-31-v1.0**

|  |  |  |
| --- | --- | --- |
| Author:  EIT O365 | Business Unit:  Enterprise IT | Classification:  Internal |
| Reviewer:  EIT Information Security, EIT, Internal Audit Group | Business Function:  IO | Status:  Draft |
| Approver: | Publish Date: | Version: 0.1 |

TABLE OF CONTENTS

[1 introduction 2](#_Toc507938210)

[2 scope 2](#_Toc507938211)

[3 Roles and Responsibilities 2](#_Toc507938212)

[4 Document Review 2](#_Toc507938213)

[5 Access Control 3](#_Toc507938214)

[Table 5‑1 Access Control 3](#_Toc507938215)

[6 Secure Configuration and Administration 3](#_Toc507938216)

[Table 6‑1 Secure Configuration and Administration 4](#_Toc507938217)

[7 Logging, Auditing and Monitoring 5](#_Toc507938218)

[Table 7‑1 Logging, Auditing and Monitoring 5](#_Toc507938219)

[8 Checklist 6](#_Toc507938220)

[9 References 6](#_Toc507938221)

[10 Appendix I 6](#_Toc507938222)

[11 Version Control 6](#_Toc507938223)

[Table 3‑1 Version Control and History 6](#_Toc507938224)

# introduction

This document represents Al-Futtaim Group Standard and associated implementation procedures for following services of O365.

* **One Drive for Business (ODFB)**
* **Exchange Online (EXO)**
* **Sharepoint Online (SPO)**

Each Standard statement comprises of:

* A Control Standard/Requirement
* An impact statement
* Implementation procedures

The **Control Standard/Requirement** specifies uniform control practices and system parameters to enforce security.

The **Impact Statement** provides the possible negative implications of not following the defined control standard.

**Implementation Procedures** are high-level concepts, provided as guidance to asset owner or data custodian who would need to perform or configure the control standards.

# scope

One drive for Business (ODFB), Exchange Online (EXO) and Sharepoint Online (SPO) deployed within Microsoft Cloud Infrastructure and controls are classified under following categories:

* Access Control
* Secure Configuration and Administration
* Logging, Auditing and Monitoring

**Compliance** with defined **Mandatory** control standards are considered necessary within the Al-Futtaim Group, unless their implementation unfavorably impacts business and operational requirements.

**Non-compliance** with Standards must be documented with **Appendix I**. Standard compliance status sheet must be submitted to the IT Compliance with non-compliance, mitigating controls, and related residual risk. The Information Security Group will review this sheet and ensure appropriate acceptance/ rejection signoffs are sought from appropriate authorities through formal exception document to avoid non-compliance.

# Roles and Responsibilities

* Infrastructure & Operations team shall be responsible for implementation of all the Controls mentioned in the standard on One Drive for Business (ODFB), Exchange online (EXO) and Sharepoint (SPO) from the publishing/last release date.
* InfoSec is responsible for controls compliance verification as per the Information Security Risk Management Framework (Refer: AFG-EIT-IG-GL-04\_Information-Security-Risk-Management-Framework).
* The Internal Audit team may refer this standard during One Drive for Business (ODFB), Sharepoint Online (SPO) and Exchange Online (EXO) Audit.

# Document Review

InfoSec must review this document at least once in a year or whenever major changes occur in One Drive for Business (ODFB), Sharepoint Online (SPO) and Exchange Online (EXO) features/controls released by Microsoft and circulate for stakeholders review.

# Access Control

This section contains standards designed to protect the confidentiality and integrity of information by introducing controls that restrict access to authorized users and limit the possibility of unauthorized access. Also address the control requirements related to legitimate user credentials, and the definition of users having similar access requirements into manageable groups.

Table 5‑1 Access Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. No.** | **Control Standard / Requirement** | **Impact if Not Implemented** | **Implementation Procedures** | **Mandatory/ Good to Have** |
| **Common Access Controls for all services of O365** | | | | |
|  | **Restrict access to the O365 group administrator portal and other administrator roles**  Access to the group admin and other admin portals need to be restricted to designated AFG administrator of Infrastructure and operations team users only | O365 administration portal with broad access to admins may lead to access by multiple users. This situation can result in configuration discrepancies. | * Enable multi-factor authentication for global administrator and other administrator roles * Leverage Azure multi-factor authentication solution for strong authentication in addition to Al Futtaim ADFS authentication to access O365 SAAS platform | **Mandatory** |
|  | **AFG End User Authentication**  AFG User should access the O365 platform using the AFG domain credentials | Unauthorized access and privileges to O365 AFG account and information. | * AFG Active Directory Federation Services (ADFS) authentication should be in place using SAML authentication when in AFG network or through AFG VPN * Any connections initiated from outside AFG network or AFG VPN need to have a Multi-factor authentication in place | **Mandatory** |
|  | **Authorized AFG Devices**  Access to O365 platform should be allowed only from AFG managed devices | Unauthorized devices access O365 AFG account and information. | * Access will be allowed only from corporate AD domain joined desktops / laptops * Mobile devices registered in AFG managed Air watch Enterprise mobility management solution will be allowed to access the O365 | **Mandatory** |

# Secure Configuration and Administration

Secure Configuration and Administration is to set the best practices recommended for controlling production configurations. By identifying, controlling, maintaining and verifying the items, make Al-Futtaim Group information administrated securely.

Table ‑ Secure Configuration and Administration

| **Sr. No.** | **Control Standard / Requirement** | **Impact if Not Implemented** | **Implementation Procedures** | **Mandatory/ Good to Have** |
| --- | --- | --- | --- | --- |
| **Common Secure Configuration and Administration Controls for all services of O365** | | | | |
| 6.1 | **Secure Channel**  All the communications to O365 SAAS platform need to be over an encrypted channel irrespective of the mode of access i.e. browser, rich client or mobile app | When communication channel is not encrypted, an attacker can carry out man in the middle attack and also get unauthorized access to AFG information | * Set up an SSL VPN or network level VPN for all communications to O365 platform irrespective of mode of access and device used and network source | **Mandatory** |
| **One Drive for Business (ODFB)** | | | | |
| 6.2 | **AFG Internal data Sharing**  Information sharing between AFG users is allowed based on the AFG information classification policy  irrespective of the mode of access i.e. browser, rich client or mobile app | AFG sensitive information can be leaked without any restriction at user, device and mode of access | * Cut-copy-paste, upload and download features to be allowed only on AFG Active directory joined systems using browser and rich clients * Sharing of files and folders with Internal users should not be allowed * For mobile apps, cut-copy-paste mechanisms including upload and download to be allowed managed by AFG Air watch-mobility application management | **Mandatory** |
| 6.3 | **AFG External data Sharing**  AFG Information, irrespective of the mode of access i.e. browser, rich client or mobile app should be disabled for ODFB | AFG sensitive information can be leaked without any restriction at user, device and mode of access | * Disable external sharing on One drive for Business | **Mandatory** |
| **Sharepoint Online (SPO)** | | | | |
| 6.4 | **Internal Access (Browser Only)**  Restricting the mode of access only to browsers for internal usage | AFG sensitive information can be leaked without any restriction at user, device and mode of access | * For Sharepoint online, only browser based access to be enabled. Mobile app and rich/sync clients must not be allowed | **Mandatory** |
| 6.5 | **External Sharing (Browser only)**  Restricting the mode of access only to browsers for collaboration activity wherein non-AFG users are involved | AFG sensitive information can be leaked without any restriction at user, device and mode of access | * SPO shall be used for external sharing, provided there is automated workflow in place for the site creation and also a workflow for designated owner approval prior to enable external sharing for a site | **Mandatory** |
| **Exchange Online (EXO)** | | | | |
| 6.6 | **Outlook Client** | AFG sensitive information can be leaked without any restriction at user, device and mode of access | * Outlook clients to be allowed from AFG domain systems only with connect with single sign on (SSO) * For outlook clients connecting from non-AFG systems, AFG ADFS and multi-factor authentication should be in place | **Mandatory** |
| 6.7 | **Outlook Mobile App** | AFG sensitive information can be leaked without any restriction at user, device and mode of access | * Access to O365 will be permitted only from policy complaint mobile devices registered in AFG Enterprise Mobile Management | **Mandatory** |
| 6.8 | **Outlook Web Access** | AFG sensitive information can be leaked without any restriction at user, device and mode of access | * Email browser access to OWA from any device will be allowed with Multi-factor authentication protection from outside AFG network | **Mandatory** |

# Logging, Auditing and Monitoring

The audit log provides the capability to investigate unauthorized activities after they occur so that proper remedial action can be taken. Auditing and monitoring standards require O365 administrators to enable mechanism to track user activities and events with the objective of identifying (and responding to) potential security incidents and/or enable timely recognition of potentially unauthorized activity of the systems(s).

Table ‑ Logging, Auditing and Monitoring

| **Sr. No.** | **Control Standard / Requirement** | **Impact if Not Implemented** | **Implementation Procedures** | **Mandatory/ Good to Have** |
| --- | --- | --- | --- | --- |
|  | **Audit Logging**  Audit trail of all the activities need to be logged and maintained | Without appropriate audit logging, an attacker's activities can go unnoticed, and evidence of whether or not the attack led to a breach can be inconclusive. | * Enable O365 audit log search and retaining of logs for at least 6 months | **Mandatory** |
|  | **Monitoring and Alerting of Administrator portal activity**  O365 global administered portal and other administrator activity needs to be monitored and altering mechanism should be in place | Administrative changes at the group level and specific application level impacts the configurations for the entire AFG O365 platform | * Create Policies that will trigger right alerts and generate sufficient logs that will support investigation during and after incident(s) | **Mandatory** |

# Checklist

It is strongly recommended to apply all the security standards mentioned explained on the above sections; the following checklist contains the consolidated list of major security standards for the convenience of O365 administrator

| **Sr. No.** | **Control Standard / Requirement** |
| --- | --- |
| 5.1 | Restrict access to the O365 group administrator portal and other administrator roles |
| 5.2 | AFG End User Authentication |
| 5.3 | Authorized AFG Devices |
| 6.1 | Secure Channel |
| 6.2 | AFG Internal data Sharing |
| 6.3 | AFG External data Sharing |
| 6.4 | Internal Access (Browser Only) |
| 6.5 | External Sharing (Browser only) |
| 6.6 | Outlook Client |
| 6.7 | Outlook Mobile App |
| 7.1 | Outlook web Access |
| 7.2 | Audit Logging |
| 7.3 | Monitoring and Alerting of Administrator portal activity |

# References

The following references have been used while developing the Standard:

* Al-Futtaim Group Information Security Policy
* Microsoft O365 Security and Compliance Centre

# Appendix I

Compliance status checklist (to be added once the control standard has been approved)

# Version Control

Table ‑ Version Control and History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version No.** | **Changed Section** | **Change Description** |
| 22nd February, 2018 | 1.0 | Initial Version | NIL |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |