365SecurityREADY™

Achieving Security & Information Protection with Microsoft 365

In this era of fast digital transformation, an organisation's most valuable asset is its data, yet many enterprises are struggling with data security and information protection as the need for cloud-based modern workplace increases.

365SecurityREADY is a pragmatic approach combining consultation and technical implementation of Microsoft 365 Threat Protection and Information Protection, in a sequence of steps that ensures most efficient and complete adoption of Microsoft 365 for an organisation.

Executed jointly with the organisations' internal IT team, The Cloud Factory 365SecurityREADY helps businesses move fast on their Microsoft 365 technical implementation, ensures complete adoption of Microsoft 365 Security & Information Protection features and empowers internal team with full knowledge transfer & support.

365SecurityREADY

365SecurityREADY scope includes deployment of following Microsoft 365 Threat Protection & Information Protection features:

	Standard protection for general organisations
Threat Protection:	
Mobile Device Management (MDM) for corporate-owned PCs and laptops	✓
Mobile Application Management (MAM) for restricting copying or saving of company data to unauthorised apps & locations, for e.g. employees cannot save organisation data on personal devices such as home PC or mobiles	✓
Enable Self-Service Password Reset (SSPR) – employees can reset their password on their own anytime, without requiring IT support	✓
Enable Multi-Factor Authentication (MFA) – put in place an additional login security layer which makes it exponentially more difficult for hackers to get access to employees' accounts	✓
Conditional Access – maintains control over how organisation data is being accessed by employees based on permitted application or their geographical location – for e.g. block specific employees who are accessing organisation data from outside home country	✓
Microsoft Defender for Office 365 – safeguards your organisation against malicious threats such as phishing attempts and ransomware, posed by email messages, links (URLs)	✓
Information Protection:	
Classify, identify & tag email and documents with sensitivity labels (such as General, Internal Only or Sensitive, etc.) to apply data protection policies (for e.g. do-not-print, do-not-forward, for internal sharing only, etc.)	✓
Data Loss Prevention on emails & documents – protects organisation sensitive data from intentional or unintentional leakage, blocking undesired actions and access by untrusted and/or malicious actors	✓
Email & documents long-term retention – enable long-term data retention policies to ensure organisation never lose an email or document due to intentional or unintentional delete by anyone and adheres to compliance requirements	✓

Contact Us

The Cloud Factory EMEA Ltd.
1, The Factory Building, Vivéa Business Park, Moka | Mauritius
T: +(230) 433 7629 | E: hello@tcf.cloud