FULCRUM DIGITAL FD

Office 365- Security and Compliance

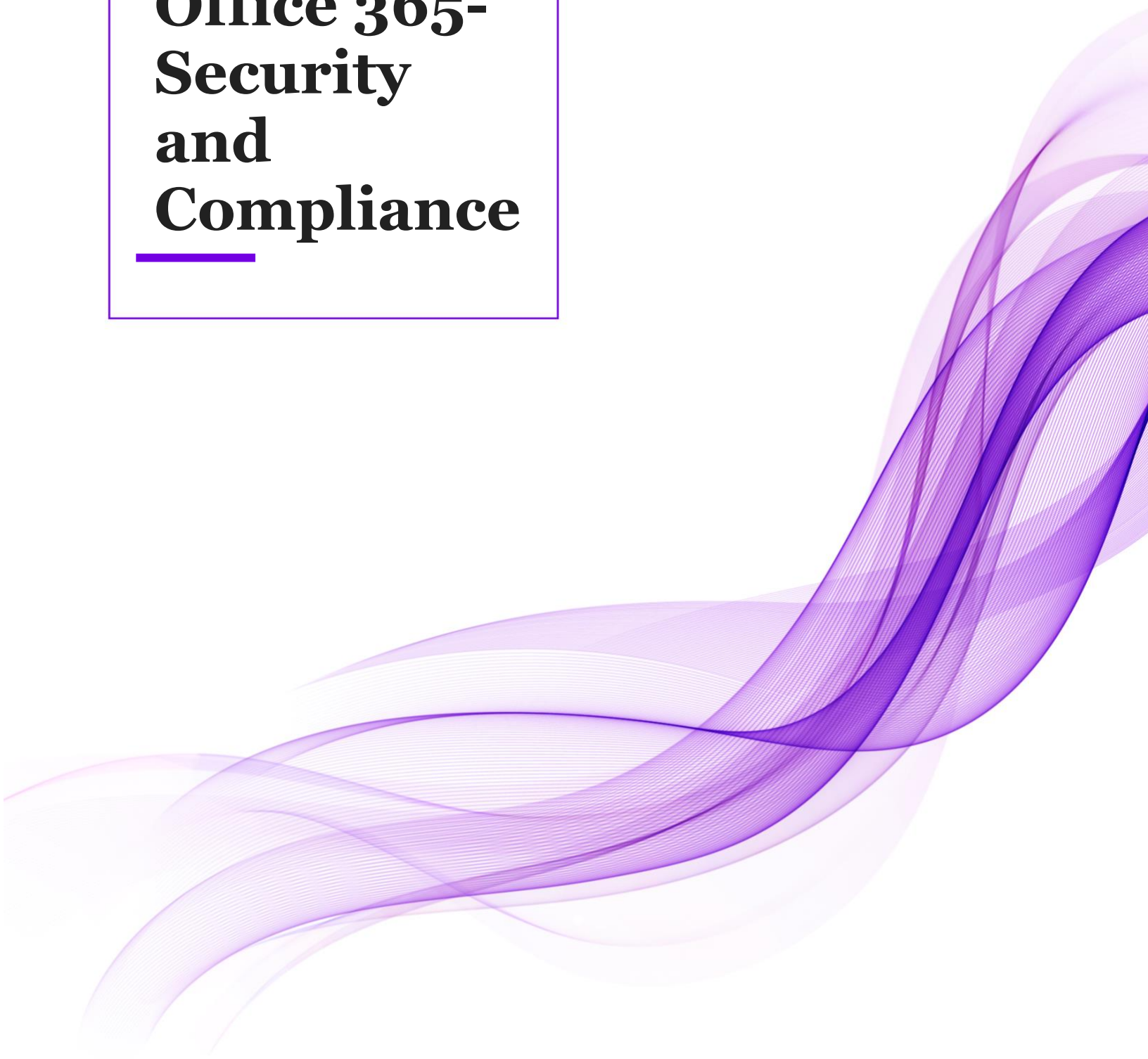

Table of Contents

1 Office 365 – Security and Compliance

1.1 General Content

It is becoming a must for almost every business that businesses can monitor and customize security elements in cloud-based productivity services like email, calendars, content management, collaboration, and unified communications. It is required to deliver more access to production services for devices, platforms, and places than ever before. Organizations must simultaneously manage the risk posed by

their users mistakenly losing or compromising essential data while also dealing with constantly changing threats worldwide.

For these reasons, organizations require a cloud service that has both

(a) integrated robust security features and

(b) Businesses can adjust various customizable security features to suit their needs.

If an organization deploys productivity services exclusively on-premises, adding this mix of security functionality may be challenging and expensive while still adhering to security best practices for remote access.

1.1.1 Microsoft Office Security

The consideration of trust is added because of security concerns while migrating your company to cloud services. The processing of "your data," which you give to the service provider when using the online service, depends on your ability to trust the service provider. In Office 365, security, compliance, and privacy have two equally crucial dimensions:

- Microsoft-managed service-level capabilities, including technologies, operational processes, and rules, are included in the first dimension and are, by default, enabled.

- The second dimension consists of customer-managed controls that let you alter your Office 365 environment per the unique requirements of your business while also upholding security and compliance.

Office 365 – Security and Compliance

2 Compliance

Compliance and security are not static but relatively continual processes. Highly qualified, knowledgeable, and trained staff members regularly maintain, improve, and verify it. Microsoft will support hardware and software innovations through reliable procedures. Microsoft uses techniques like the Security Development Lifecycle, i.e., methods that throttle traffic and prevent, detect, and remediate breaches, to help keep Office 365 security at the top of the sector.

2.1 Service Level Security

Microsoft is the market leader when it comes to cloud security. To deliver a secure cloud productivity service that complies with industry standards for compliance, the company draws on its decades of experience in developing enterprise software and operating online services and its ongoing commitment to learning and updating the services and applications.

At the service level, it uses a defense-in-depth strategy that protects the data through multiple layers of security (physical, logical, and data):

A. A defense-in-depth approach ensures security measures are in place at multiple service levels and that, should one area fail, there are backup measures to keep security up.
B. The plan also outlines techniques for anticipating, detecting, and mitigating security breaches. Below are service-level security features, including:
    - Port scanning and remediation
    - Perimeter vulnerability scanning
    - OS patching
    - Multi-factor authentication

2.2 Built-in Security

24-Hour Monitored Physical Hardware:

The worldwide Microsoft network of data centers stores information from Office 365. These data centers were designed from the ground up to safeguard services and information against damage from natural disasters or unwanted access.

Only necessary staff have access to customer applications and services because data center access is regulated by job function around-the-clock. Multiple identifications and security procedures are in

place for physical access control, including badges and smart cards, biometric scanners, on-site security guards, ongoing video surveillance, and two-factor authentication.

Motion detectors, video surveillance, and security breach alerts monitor the data centers. If necessary, seismically braced racks and automated fire prevention and extinguishing systems are included in the security measures for when a natural disaster strikes.

Isolated Customer Data:

Office 365 is a multi-tenant service. Through Active Directory's organizational structure and features created primarily to support the creation, administration, and security of multi-tenant settings, data storage and processing for each tenant is separated.

Active Directory isolates its users (also known as silos) by using security barriers that protect a customer's data so co-tenants cannot access or compromise it.

Secure Network:

Critical back-end computers and storage equipment are physically separated from the user-facing interfaces by segmented networks within the Office 365 data centers. Security features on edge routers make it possible to spot intrusions and symptoms of vulnerability. Outlook, Outlook Web App, Exchange ActiveSync, POP3, and IMAP client communications to Office 365 are secured using SSL. Users' Internet-capable locations serve as the starting point for customer access to services delivered via the Internet, which concludes at a Microsoft data center.

These connections are encrypted utilizing the secure sockets layer (SSL) and transport layer security (TLS) standards (SSL). The usage of TLS/SSL creates a very secure client-to-server connection between the desktops and the data center, assisting in maintaining data confidentiality and integrity. Customers can set up TLS for both inbound and outbound email traffic between Office 365 and external servers. This feature turns on by default.

Encrypted Data:

Office 365 has two states for customer data: at rest on storage media and in transit from the data center to a consumer device across a network. All data is encrypted.

Additionally, S/MIME (secure/multipurpose Internet mail extensions) messages are transported and stored by Office 365. Messages encrypted using client-side, third-party encryption tools like PSG will be transported and held by Office 365.

2.3 Admin Controls

Microsoft Exchange Online, Microsoft SharePoint Online, and Microsoft Teams are all included in Office 365, which combines the well-known Office suite with these services on the cloud. Each of these services has customizable security options that the administrator can manage. With these controls, administrators can meet compliance standards, grant access to services and content to members of an organization, set up anti-malware/anti-spam protection, and encrypt data using keys.

Enabling Advanced Encryption:

Office Professional Plus integrates with the Windows Cryptographic Next Generation (CNG) APIs to provide advanced protection with native support for Cryptographic Agility. Administrators can specify the cryptographic techniques to encrypt and sign documents.

Single Sign-On Security Provisions:

The identity platform for Office 365, Windows Azure Active Directory, allows administrators to federate on-premises Active Directory or other directory stores. Once federation is set up, all Office 365 users with their identities based on the federated domain can log in to Office 365 using their current corporate logon. Secure, token-based authentication is made possible by the federation. This also allows additional authentication methods such as:

- Two-factor authentication
- Client-based access control and location-based control (for example, limiting access from public computers or public open Wi-Fi)
- Role-based access control, like the access control procedure described above in the Automated Operations section for Microsoft personnel

Enabling Compliance:

Data loss prevention (DLP), eDiscovery, and auditing and reporting capabilities are just a few of the compliance features offered by Office 365. The user experience is maintained, and productivity is unaffected across various capacities, increasing user acceptance.

- Data Loss Prevention (DLP)

While malware and targeted attacks can result in data breaches, most organizations' primary source of data risk is user mistakes. Data loss prevention (DLP) technology from Exchange Online lets users comprehend and control data risk by identifying, monitoring, and protecting critical data. Administrators can choose the appropriate number of limits for their organization and have access to a comprehensive range of controls.

- Auditing and Retention Policies

Customers can record events, including reading, changing, and deleting content, thanks to Office 365 auditing standards, incorporating calendars, discussion groups, task lists, problem lists, emails, and documents. When auditing is activated, Administrators can view the audit data and provide an overview of current usage as part of an information management policy.

Administrators can use these reports to monitor information inside the organization, assess compliance, and look into potential problems.

- eDiscovery

To undertake e-discovery duties, the new, user-friendly eDiscovery Center can be assigned to specialized users, such as compliance officers or human resources staff, without adding extra workload to the IT department. Admin can retrieve content via eDiscovery from file shares, Exchange Online, and SharePoint Online. Admins enjoy a single experience for searching and archiving email, documents, and site mailboxes with the integrated Office 365 eDiscovery. Admins can be very particular about what they want to search for and keep using eDiscovery.

Enabling Anti-Spam/Anti-Malware:

The spam confidence level (SCL) is a value that Office 365 sets after evaluating received communications. The gateway deletes messages with high SCL values, whereas messages with low SCL values are sent to users' inboxes. Messages with SCL levels on edge are sent to users' Junk Mail folders, which remain for 30 days before being automatically deleted.

Advanced junk mail settings, organization-wide safe and blocked sender lists, and other anti-spam/anti-malware controls can all be managed by administrators using the Office 365 Administration Center. Individual users can manage their safe and blocked senders from their inboxes in Microsoft Outlook or Microsoft Outlook Web App.

2.4 Independent Verification and Compliance

Office 365 has operationalized security into a scalable process that can easily change to meet the needs of various industries. Microsoft builds and maintains a security control structure that complies with current requirements and regularly engages in risk management evaluations. The Office 365 service lifecycle includes internal and external audits by reputable organizations. The consequence of close collaboration with other Microsoft teams is a thorough strategy for protecting cloud-based apps. Office 365 meets below standards:

ISO 27001:

Office 365 is the first significant business productivity public cloud service to implement stringent international standards, including physical, logical, process, and management controls. Office 365 was developed to ISO 27001 requirements.

FISMA:

Multiple federal agencies have granted Office 365 modest FISMA Authority to Operate. Operating under FISMA necessitates openness and regular security reporting to our US Federal clients. For the benefit of clients who are exempt from FISMA standards, Microsoft implements these unique procedures across our infrastructure to strengthen our Online Services Security and Compliance programs.

HIPAA BAA:

The HIPAA BAA is now available to all users of Office 365, the first significant business productivity public cloud service provider. HIPAA is a law that applies to healthcare organizations and mandates that all covered entities sign governing protected health information (PHI). Contracts with their suppliers with access to PHI are business associate agreements.

EU Model Clauses:

The standard contract language, referred to as the "EU Model Clauses," was designed by the European Union, and Office 365 became the first significant business productivity public cloud service provider to sign it with every client.

Businesses today want productivity offerings that enable people to complete more tasks practically from anywhere while preserving security against ever-changing threats. Office 365 provides a highly secure, cloud-based work environment that simultaneously meets both demands. The Office 365 Trust Center contains information on Office 365 security, privacy, compliance, transparency, and service continuity. Every aspect of the Office 365 platform, from application development to physical data

centers to end-user access, incorporates security. Today, fewer, and fewer organizations can maintain an equivalent level of security on-premises at a reasonable cost.

Importantly, Office 365 applications offer administrators the freedom to configure, administer, and integrate security in ways that make sense for their business needs. Built-in security capabilities in Office 365 applications make it easier to protect data. When enterprises pick Office 365, they get a partner that genuinely comprehends their security requirements and is respected by businesses of all sizes in almost every sector and location.

For more information and details, please feel free to reach us at marketing@fulcrumdigital.com and our Azure expert will be in touch with you.

About Fulcrum

Fulcrum Digital is a leading IT services and business platform company. We partner with global companies from diverse industries, including banking and financial services, insurance, higher education, food services, retail, manufacturing, and eCommerce. With expertise in digital transformation, machine learning, and emerging technologies, we offer a consulting-led, integrated suite of enterprise-grade software products, services, and solutions.

www.fulcrumdigital.com

FULCRUM DIGITAL FD.