



---

System and Organization Controls (SOC) 3 Report

**Management's Report of Its Assertion on the  
Effectiveness of Its Controls Over the Workplace from  
Meta Product Based on the Trust Services Criteria for  
Security, Availability, and Confidentiality**

For the period January 1, 2021 through December 31, 2021

---

# Workplace from Meta Product

## TABLE OF CONTENTS

|  |    |
|--|----|
| Section I – Report of Independent Accountants .....  | 3  |
| Section II – Management’s Report of Its Assertion on the Effectiveness of Its Controls over the Workplace from Meta Product Based on the Trust Services Criteria for Security, Availability, and Confidentiality ..... | 6  |
| Attachment A – Workplace from Meta Product .....   | 8  |
| Scope and Purpose.....   | 9  |
| Company and Business Overview .....  | 9  |
| Workplace from Meta Product Overview .....   | 9  |
| Technology Stack .....   | 11 |
| Workplace Instance.....  | 15 |
| Relevant Aspects of the Control Environment, Information and Communication, and Monitoring Controls .....  | 18 |
| Product Environment.....   | 21 |
| Procedures.....  | 23 |
| Complementary User Entity Control Considerations .....   | 41 |
| Attachment B – Principal Service Commitments and System Requirements .....   | 43 |
| Principal Service Commitments and System Requirements .....  | 44 |
| Attachment C – Workplace from Meta, General Data Protection Regulation (“GDPR”), Security Notifications, and Data Transfer .....   | 45 |

---

## **Section I – Report of Independent Accountants**

---

## Report of Independent Accountants

To the Management of Meta Platforms, Inc.

### Scope

We have examined management's assertion, contained within the accompanying "Management's Report of Its Assertions on the Effectiveness of Its Controls Over the Workplace from Meta Product Based on the Trust Services Criteria for Security, Availability, and Confidentiality" (Assertion), that Meta's controls over the Workplace from Meta Product (System) were effective throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

### Management's Responsibilities

Meta's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Workplace from Meta Product (System) and describing the boundaries of the System
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the system
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements

### Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Meta's relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Meta's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

The description of the boundaries of the System, which is presented in the accompanying “Attachment A - Workplace from Meta Product” (Description) indicates Meta’s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Meta’s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

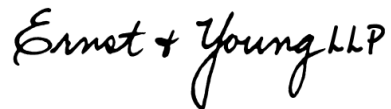
The information in the accompanying “Attachment C - Workplace from Meta, General Data Protection Regulation (“GDPR”), Security Notifications, and Data Transfer” is presented by management of Meta to provide additional information and is not part of the Description. Such information has not been subjected to the procedures applied in our examination and, accordingly, we express no opinion on it.

#### *Inherent limitations*

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Meta’s principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

#### *Opinion*

In our opinion, Meta’s controls over the system were effective throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.



May 4, 2022

---

**Section II – Management’s Report of Its Assertion on  
the Effectiveness of Its Controls over the Workplace  
from Meta Product Based on the Trust Services  
Criteria for Security, Availability, and Confidentiality**

---

## **Management's Report of Its Assertions on the Effectiveness of Its Controls Over the Workplace from Meta Product Based on the Trust Services Criteria for Security, Availability, and Confidentiality**

We, as management of, Meta Platforms, Inc ("Meta") are responsible for:

- Identifying the Workplace from Meta Product (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

Management of Meta Platforms, Inc.

---

## **Attachment A – Workplace from Meta Product**

---





## Scope and Purpose

This System and Organization Controls ("SOC") 3 report is an examination of the internal controls of Meta Platforms, Inc.'s, previously Facebook, Inc., (herein referred to as "Meta", "the Company" or "Management") Workplace from Meta Product relevant to the Security, Availability, and Confidentiality trust services criteria as set forth in TSP section 100 of the 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy established by the American Institute of Certified Public Accountants ("AICPA"). The examination was conducted by an independent service auditor in accordance with the Statement on Standards for Attestation Engagements 18 ("SSAE18") issued by the Auditing Standards Board ("ASB") of the AICPA (i.e., the relevant professional standards). Additionally, the examination was conducted in accordance with the International Standard on Assurance Engagements 3000 ("ISAE3000"), Assurance Engagements Other than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board ("IASSB").

This section of the report was prepared by the management of Meta in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and is intended to provide user organizations with information about the Workplace from Meta Product's relevant internal controls to achieve the service commitments and system requirements based on the applicable trust services criteria for Security, Availability, and Confidentiality throughout the period January 1, 2021 to December 31, 2021. It does not and is not intended to encompass all aspects of the services, procedures, or controls performed by Meta.

## Company and Business Overview

Meta (formerly Facebook, Inc.) is a publicly traded U.S. company headquartered in Menlo Park, California, with approximately 175,000 employees as of December 2021. Established in February 2004, the Company is a social networking service and website that aims to make the world more open and connected. People use Meta to stay connected with their friends and family, and to express what matters to them and to the people they care about. Developers can use the Meta Platform to build applications ("apps") and websites that integrate with Meta to reach its global network of Meta users and to build products and services that are more personalized, social, and engaging.

## Workplace from Meta Product Overview

### Background

Workplace from Meta is an enterprise communication and collaboration product that combines next-generation technology and easy-to-use features to transform communications, culture, and workflows inside organizations of all shapes, sizes, and industries. Workplace is built on Meta's infrastructure, but it is a separate platform.



Workplace allows an enterprise to establish and manage their own individual instance of Workplace. These instances, called “Workplaces” or “Communities”, allow their employees to connect and collaborate via the same core Facebook features: Groups, Messaging, Timeline, News Feed, and Events. All data that is created within this instance of Workplace or by any profile associated with it, is then contained within the boundaries of the community. Workplace also connects with other popular enterprise tools so your team can get work done faster.

Meta offers a base plan of Workplace Core with additional add-on packages.

Unless otherwise noted, references to “Workplace” in this report refer collectively to the Workplace Core product and any add-ons. In addition, the scope of this report and the controls described herein are applicable to all Workplace pricing plans unless denoted otherwise.

## **Development and Management**

Development and management of Meta’s systems, including the Workplace from Meta Product follow standards that are focused on security, availability, and confidentiality. At Meta, security, availability, and confidentiality encompass a number of key control measures:

- Access to data is controlled based on the agreements that Meta has with the individuals, businesses or organizations using the product. Access measures are in place to protect data in accordance with security and confidentiality commitments within these agreements.
- Data from different “Workplace from Meta” instances is segregated using the instances’ unique identifier associated with that instance.
- Measures are in place to collect, use, retain, and dispose of data in accordance with security and confidentiality agreements.
- Data is protected against theft or misuse.
- Processes and controls are in place to inhibit, detect, or respond to malicious activity, both internally and externally.
- Compliance with security and confidentiality policies and procedures is monitored on an ongoing basis.
- Security is part of the culture of Meta which is driven by the dedicated Meta Security team and sponsored by the Company’s senior leadership.

Meta systems and networks are maintained by highly resilient infrastructure, which is built to withstand catastrophic events. Data is replicated across geographic regions to maintain and manage recoverability and availability. Workplace uses Meta’s proprietary Domain Name System (“DNS”) architecture that takes various sources of information like capacity, resolvers and latency, routing, and health information to decide as to which globally distributed Point of Presence (“PoP”) and/or Datacenter to connect a user for maximum performance.

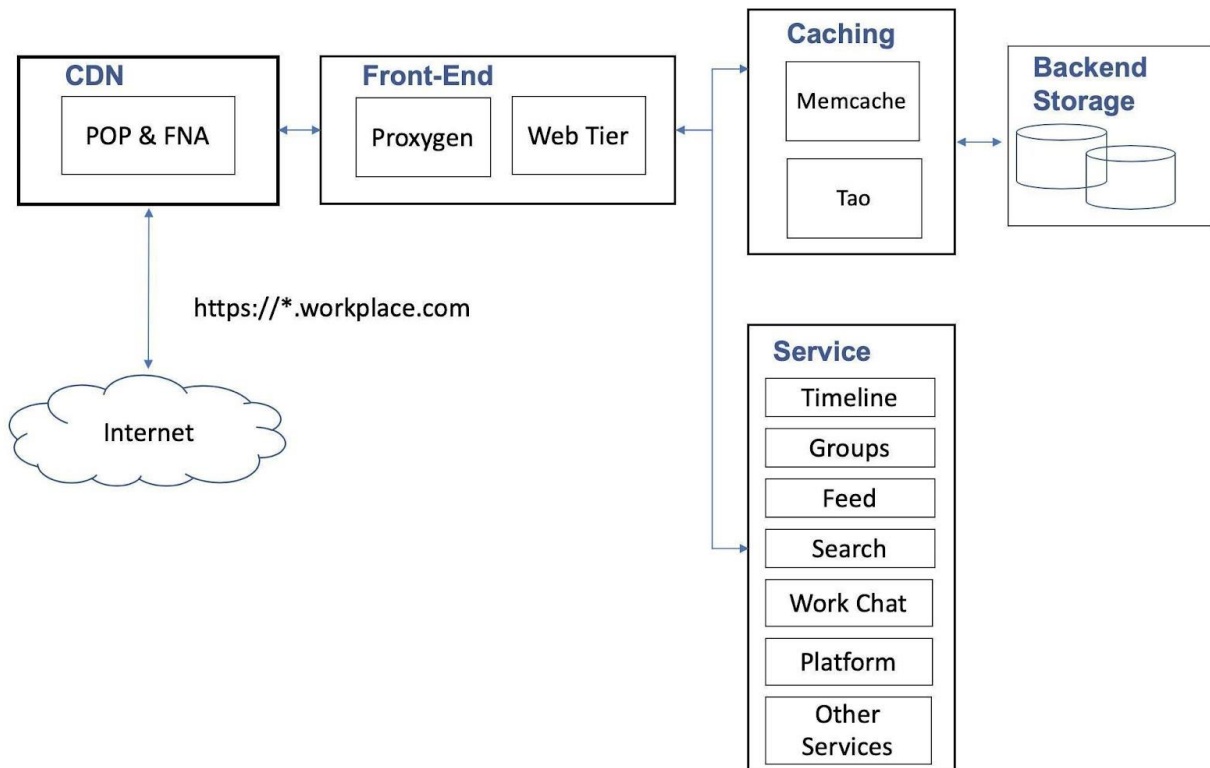


# Technology Stack

## Infrastructure

“Workplace from Meta” is an extension of the main Meta web application with additional logical privacy barriers built in to protect and maintain the confidentiality of enterprise data. The infrastructure that underlies “Workplace from Meta” has five key components:

1. Content Distribution Network (“CDN”)
2. Front-End
3. Caching
4. Service
5. Backend Storage



*Figure 1: Workplace from Meta Components*

Each of these components consists of clustered Linux servers running a combination of open source and custom-built software. Workplace infrastructure is the same as Meta’s web (“www”) environment. Within this environment, “Workplace from Meta” data is stored on the same servers used to store data originating from Meta’s www platform, and thus, inherits the same security controls. To further protect the data of organizations using “Workplace from Meta”, Meta segments “Workplace from Meta” data through the strict security controls described in the Managed Communities section below.



### *Content Distribution Network (“CDN”)*

Internet to Meta traffic is mainly comprised of two types of requests: dynamic (i.e., requests for Messages (delta), Timeline, Feed, Groups, Search, or other services) and static requests (i.e., requests for images, videos, or other static content). To handle the large volume of requests while maintaining a performant experience for users, Workplace uses a Meta owned and operated Content Distribution Network (“CDN”). This CDN includes several layers of cache including Edge Point of Presence (“PoP”) and Fabulous Network Appliances (“FNA”, i.e. Meta-owned and protected network appliances deployed at ISPs), which are not considered in-scope locations but do transmit encrypted data to Meta-owned data centers. Use of this high performing multi-tier cache enables Workplace to deliver static files such as photos and videos to users faster.

Each PoP and FNA houses Meta equipment to either fulfill the request itself or direct the request to the closest Meta data center to retrieve the specific services and content.

### *Front-End*

Meta’s front-end is responsible for receiving and responding to requests made by enterprise users by way of the CDN and Meta data center Proxygen servers. Running Hip Hop Virtual Machines (“HHVM”), Meta’s open-sourced web server and code execution engine, these web servers interface with the Proxygen servers to receive and respond to requests on the front-end while also interfacing with the caching, service, and backend data storage components to receive the requested services and data. The front-end is primarily comprised of servers that render the Workplace server-side code and orchestrate loading the various services (i.e., Timeline, Feed, Groups, and Search) when an enterprise user requests them.

### *Caching*

To reduce latency and retrieval times, “Workplace from Meta” utilizes caching to provide data to enterprise users. When receiving a request from the front-end or service tier, the caching tier will first look to see if it can provide the data from its cache. If it cannot, it will make a request to the data storage tier to retrieve the specific data.

The caching component is comprised of two major systems: Memcache and TAO.

Memcache stores data in system memory and is optimized for reads-over-writes since enterprise users typically consume more data than they produce. Consequently, content is readily available when an enterprise user requests it. Memcache is a general-purpose cache that is distributed across the front-end clusters and stores data such as the results of API and database calls to limit network, database, and disk load to more efficiently respond to the billions of requests received per second. While Memcache is primarily used to store and retrieve general-purpose data objects, TAO is used to store graph data. Graph data consists of FBOjects, such as users, posts, groups, and associations (“assocs”), such as likes, between the FBOjects.

TAO makes up the other major component of Meta’s caching and is originally derived from Memcache, so their primary function of reducing latency and retrieval times along with their architecture are the same. However, TAO is the primary mechanism for storing, caching, and querying graph data.



Refer to the Managed Communities section that follows for more information on assoc.

### *Services*

The service component consists of the services Workplace provides such as Timeline, Feed, Groups, Messaging, and Search. Standard services have dedicated clusters and computing resources to deliver the specific service to the enterprise user. The design and architecture of each service's infrastructure is optimized to fulfill the service's purpose. For example, Timeline is responsible for displaying an enterprise user's posts, and posts an enterprise user is tagged in. This requires specific methods to rank relevant posts the enterprise user is interested in. On the other hand, Search may require a different architecture to index and quickly search through posts, groups, and users while returning relevant results quickly after the enterprise user requests them.

### *Backend Storage*

As enterprise users create dynamic content (i.e., create posts), their data is stored within clusters of geographically distributed MySQL databases housing user-generated content and data. When enterprise users request access to data, their request first hits the cache, and if not fulfilled, it hits backend storage for retrieval. "Workplace from Meta" leverages Meta's highly available, optimized binary large object ("BLOB") storage solution to store customer static content such as photos and videos.

### **Software**

Enterprise users may interact with the Workplace environment through the web interface (<https://company.workplace.com>), the mobile site (<https://company.m.workplace.com>), or the "Workplace from Meta" mobile applications. Administrators are able to interact with Workplace for management of the community through the Company dashboard and Workplace APIs. The software that provides user interfaces for the Workplace product is comprised of five main components:

1. Web ("www")
2. Mobile Applications ("apps")
3. Company dashboard
4. Workplace from Meta Account Management Application Programming Interfaces ("APIs")
5. Workplace from Meta Product (Integrations)

Workplace administrators must provision Workplace profiles with the necessary access rights for their users before they can use any of these interfaces.

### *Web ("www")*

The www interface is accessible through traditional web browsers and is one of the primary ways an enterprise user accesses Workplace. Workplace looks and feels the same as Meta and allows enterprise users to have a similar experience of viewing their Timeline, interacting with friends (work colleagues within the managed community), and sharing posts, photos, and videos, while also being able to participate in group conversations and schedule company events.



### *Mobile and Desktop Applications*

Workplace chat mobile applications are available for iOS and Android operating systems. The mobile applications allow users to use all supported Workplace features and functionality through their mobile devices. The mobile applications connect to the Workplace infrastructure described above over an encrypted API connection using Transport Layer Security (“TLS”) certificates for in-transit data. Similarly, desktop workplace chat applications are available for Windows, Mac, and Portal from Meta.

### *Company Admin and Security Dashboard*

The company dashboard is a front-end user interface residing within each Workplace managed community. Within this portal, Workplace admins can manage community settings, user access, and content.

The security dashboard provides admins with logs and visibility into overall security health based on the security events identified. It shows login, password, admin, file, and third-party app integration activity. The same technology that powers Meta to detect and block malicious files and URLs is enabled for Workplace instances.

Within the company dashboard, admins can allow enterprise users to download a copy of their Workplace data (“DYI”) such as profile information, posts, or chat messages to meet their regulatory requirements.

### *APIs*

Enterprises have access to two primary APIs that are used to manage users and data within the community:

- *Workplace from Meta Account Management API* is a System for Cross-domain Identity Management (“SCIM”) which allows administrators to manage enterprise users, including creation of users, user groups, and removal of users adhering to the SCIM standard.
- *Workplace from Meta Graph API* allows administrators to interact with and manage data in the community programmatically.

Enterprises own and administer their Workplace instance data. Enterprises can modify, delete, or export their data at any time. Meta’s industry standard APIs allow for real-time activity monitoring and content exports.

### *Platform*

The Workplace Product provides company admins the ability to integrate and configure third-party applications with Meta’s Workplace instance. Platform enables this by providing apps access to company data through a number of APIs. The three types of integrations provided by Workplace Platform are:

- First-Party - built by Meta
- Third-Party - built by a (verified) partner
- Custom Integrations - built / operated by the customer





Workplace system administrators can control the capabilities offered to each integration by creating apps and granting them specific permissions. Each app can be named to reflect the service it enables. Apps come with unique access tokens and permissions to control what information is allowed to be read or written by that app.

Third-Party Apps allow Independent Software Vendors (“ISVs”) to integrate their System-as-a-Service (“SaaS”) and Platform-as-a-Service (“PaaS”) products with Workplace. Once reviewed and approved by the Workplace team, these apps can then be installed by any Workplace community administrator to deliver valuable automation.

## **Workplace Instance**

### **Defining an instance**

When a company signs up for Workplace, Meta creates a community ID supporting the Workplace instance. All subsequent data produced within the instance or by any profile associated with the instance will be retained within the boundaries of the instance. The user’s profiles that are used to access the instance are unique to that instance and separate to a user’s Meta account. These boundaries restrict the ability to access and view content to only those users that belong to the instance; thus, no content is publicly accessible. The company may also choose to further restrict access to company content through the use of company-specific groups (i.e., only certain members/employee accounts may be able to access the group).

To enforce the confidentiality boundaries, Meta utilizes an Entity (“Ent”) framework. These Ent’s act as objects that allow “Workplace from Meta” data to be organized by instance. In addition, when an enterprise user has a relationship with an object (i.e., creates a post, likes an object, etc.), an association (“assoc”) or link is created between the enterprise user and the activity/object. Assocs are also utilized to help ensure that relevant content for each company is displayed appropriately, limiting viewing and editing rights to those users that belong to the instance and have rights to interact with the specific content in the request.

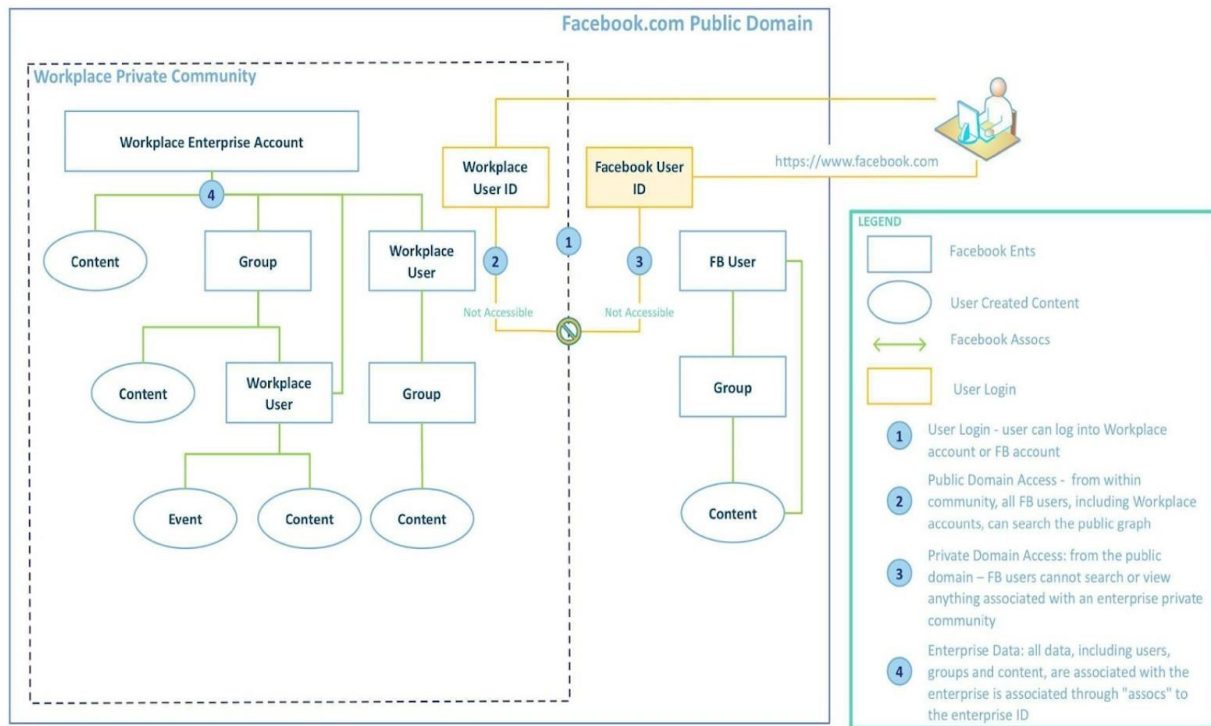


Figure 2: Ents and Assocs

## Instance Management

### Initial User Setup

After a company signs the Workplace contract, a Workplace instance gets created, after which, additional company administrators and employees of the company may be onboarded.

Company administrators can utilize the SCIM-compliant API to perform create, read, update, and delete functions for users. Administrators can create new profiles, delete enterprise user profiles, create and manage groups, and import organizational hierarchies. The SCIM API also allows for linkage to third-party cloud identity services. Company administrators can add, delete, and modify users and groups through the company dashboard within “Workplace from Meta”.

Workplace is built to give everyone in customer organization a voice, whether they work in the head office or on the factory floor. Meta recognizes that not every employee is given a corporate email address, which has been the traditional way of sharing activation links and because of that, Workplace has created access codes as a method of provisioning accounts. With these access codes, employees can activate their account without the need to have a corporate email address. Companies can enable better frontline user management and experience using specific features, such as email-less user accounts and Areas (which are collections of people who belong to common criteria, like a location or a cost center).





Once a new Workplace profile is provisioned, an employee will receive an email inviting them to activate the respective “Workplace from Meta” profile. Workplace user profiles are not linked to or associated with an individual’s personal Meta account.

#### *End User Management*

Once an instance has been created by Meta, instance administrators are responsible for performing all management functions of the Workplace community. Instance administrators are expected to manage user-generated content, provision and deprovision users, modify community settings, manage groups, and access community insights/statistics.

Users can submit support requests through the Direct Support Channel in the Workplace Admin Panel. The initial response windows are within 4 hours for customers with the Enhanced Admin and Support add-on and 24 hours for Core customers. These times are calculated from when the email confirmation is received that a support ticket is raised.

#### *Data Management*

The data gathered from Workplace will be gathered on behalf of the company signed up to use Workplace as a service. User-generated content contained within the company’s instance, as well as logged user activity, is stored on Meta’s servers until the end of the Workplace service contract or until the company decides to delete the data. Meta does not provide any archiving service, and the customer is solely responsible for creating backups of their data.

Instance admins may delete groups, the instance’s user-generated content, or the customer’s entire Workplace instance. Once the option to delete this data is confirmed, the data will be deleted in alignment with Meta’s data deletion policies. Companies also have the option and ability to access, correct, backup, or delete any relevant data via the “Workplace from Meta” API. Further, company data is not collected or utilized for the purposes of advertising by Meta.

#### *Multi Company Groups and Chats*

A special instance type, ‘multi company groups’, exists within Workplace. This is a shared group that allows employees from one company to collaborate in a group with employees of another company, as long as the employee has a Workplace profile. By default, the group creator is the admin for a multi-company group. Multi-company chats (“MCCs”) allow people in multi-company groups (“MCGs”) to chat, video, and voice call in 1:1 or group threads.



## Relevant Aspects of the Control Environment, Information and Communication, and Monitoring Controls

### Control Environment

Meta protects the confidentiality, integrity, and availability of data stored on its systems, platforms, and products (“Information Systems”) through its Comprehensive Information Security Program (“CISP”). The CISP is specifically designed and scoped to address Meta’s unique Information Systems and business needs, including controls appropriate to Meta’s size and complexity, the nature and scope of Meta’s activities, and the sensitivity of the user information Meta processes and stores.

### Comprehensive Information Security Program

#### *Roles and Responsibilities*

Meta regards security as a company-wide responsibility, training all of its personnel on relevant security requirements, and providing tools to develop and maintain secure products and services. Meta’s security efforts are overseen by the Security Team, which has the primary responsibility to implement and maintain Meta’s CISP. This responsibility encompasses designing, developing, implementing, and maintaining security safeguards, including policies, standards, and guidelines. Security Team members provide services in four core functions:

- **Prevention**, inhibiting the ability of attackers to compromise Meta’s Information Systems;
- **Detection and response**, tracking, analyzing, and monitoring risks to Meta’s Information Systems;
- **Measurement and validation**, evaluating the effectiveness of Meta’s security safeguards; and
- **Programs and operations**, supporting the delivery and enhancing the effectiveness of the security work performed across Meta, including providing resources to Meta Personnel to support creation of products that are secure by design.

The Security Team is led by a Vice President, Engineering, who also oversees the implementation of the CISP and has direct reporting authority and obligations to Meta’s Board of Directors.

Meta’s Board of Directors (“BOD” or “Board”) has adopted Corporate Governance Guidelines, which assist the Board in the exercise of its governance responsibilities and serves as a framework within which the Board may conduct its business. Within the BOD, an Audit Committee has been established and is independent of management. The Audit Committee is charged with oversight of the company’s management of risk, accounting and financial reporting processes, and the audits of the financial statements of the Company, as well as the independence, qualifications, and performance of the



independent audit. The authority, roles, and responsibilities of the Audit Committee are governed by a charter, which is reviewed by the Audit Committee.

Information Security Risks or updates are discussed with the Audit Committee/Board of Directors by Meta senior leadership on at least an annual basis.

The Security Team manages and provides overall guidance of the security policies and procedures that affect the security, availability, and confidentiality of information. These policies and procedures are reviewed at least annually and updated as needed. Significant changes to the Information Security Policy are communicated to senior management and employees through Meta groups dedicated to security. The most up-to-date policies and procedures are available to personnel via Meta's intranet.

### *Security and Confidentiality Policies*

Various security policies are in place that have been approved by management and made available to employees and cover a variety of areas. Meta divides these policies into the following major categories:

- Application Security
- Asset Management
- Business Continuity and Disaster Recovery
- Change Management
- Configuration Management
- Data Security
- Identity and Access Management
- Logging and Monitoring
- Network Security
- People Security
- Physical and Environmental Security
- Security Incident Response
- Security, Compliance, Policy and Risk
- Third-Party Security
- Vulnerability Management

Policies within each of these areas create the overall framework that Meta uses to secure systems across the environment. Responsibility and accountability for management of Meta's system security and confidentiality policies lies with the Security Team. The Security Team is also responsible for partnering with various teams within the Company to implement these policies.



## **Internal Audit**

On an annual basis, the Internal Audit (“IA”) team meets with different teams within Meta such as the Security Team, Legal, Tax, etc., to understand threats to Meta from each team’s perspective. The IA team takes a risk-based approach to prioritize the projects and activities that would be addressed in each half of the year. The IA team also prepares a risk-based audit plan for the following year. The annual internal audit plan is presented to and approved by the Board.

## **Monitoring of Controls**

Management is responsible for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Management places an emphasis on maintaining sound internal controls and the integrity and ethical values of Meta personnel. The Company’s values and behavioral standards are communicated to personnel through training and policy statements.

Various logging and monitoring applications are in place to mitigate the risk of unauthorized access. In addition, monitoring of performance, quality, and adherence to Company policies and internal controls is part of the day-to-day responsibilities of management. Meta uses several specialized tools to monitor the Company environment. This monitoring includes components for detecting:

- Intrusions by malicious threat actors
- Violations of security and confidentiality policies and procedures by employees
- Changes to systems and configurations
- Vulnerabilities in Meta systems
- Issues with the operational health of systems

There are designated on-call teams responsible for monitoring and resolving security incidents, depending on the type of incident or violation.

In addition, management conducts several compliance audits (SOC 2, SOX, PCI, ISO 27001, ISO 27018) and other non-compliance audits to ascertain that appropriate controls are in place and are operating effectively to mitigate identified risks. Furthermore, the Security Team reviews the control environment and the implemented controls to help ensure that appropriate controls are in place to mitigate identified risks.

## **Information and Communication**

### *External Communication*

A description of Meta’s systems and services is available to users through the Meta website. Meta communicates the security, availability, and confidentiality obligations and commitments for external users and internal users via multiple methods and channels. These channels include the "Terms of Service" and "Data Policy", which are available on the Meta Terms and Policies page and help center. There is also a formal process for contacting Meta with questions and concerns, which is communicated to users through Meta’s security page (<https://www.facebook.com/security>).



### *Internal Communication*

Meta uses various methods of communication to help employees understand their individual roles and responsibilities and to communicate events in a timely manner.

Policies and procedures are in place for employees and these policies are made available to employees through the Meta intranet. Prior to employment, offer packets are sent to employees, which include employment contracts and confidentiality agreements. Employees must sign confidentiality agreements as a condition of employment. Orientation packages are provided to newly hired employees and include training on security, availability, and confidentiality obligations, ethics, and relevant policies and procedures.

The Security Team conducts several company-wide security awareness activities, including National Cyber Security Awareness Month, and periodic security awareness campaigns to reinforce the Information Security practices and policies. The results of these activities are documented and communicated to employees to increase their awareness and ability to respond to threats and vulnerabilities.

The company has established on-call procedures for the response and resolution of security incidents. These procedures are made available to Security Team members through security Wiki pages.

Substantive changes to security policies are communicated to senior management and Meta employees via internal Meta groups. The Security team conducts regular all-hands meetings to update Security Team members on new security threats and environmental, regulatory, and technological changes that may impact security.

## **Product Environment**

### **Organizational Structure**

#### *Product Teams*

Product Teams are cross functional teams composed of individuals from within the broader Meta organization that specialize in designing, developing, implementing, operating, maintaining, and monitoring each respective product to meet Meta's security, availability, and confidentiality commitments. The Product Teams lead the development, maintenance, and growth of each respective product. The Product Teams are comprised with following key roles:

- **Product Manager:** Lead at the Meta organizational level, who determines the ongoing strategy and growth of each respective product.
- **Engineering Manager:** Lead responsible for coordinating all software engineering efforts across each platform (www, iOS, Android, etc.).

The Product Manager and Engineering Manager coordinate the design, development, implementation, operation, maintenance, and monitoring efforts of each respective product with employees from across the Meta organization including the following:



- Engineering: Pulled from the existing Meta engineering groups but specializing in the respective product. The team is divided by platform (web, iOS, Android, etc.) and supports the Product Development Team with the operation and maintenance of each respective product.
- Security Partner: The dedicated security partner builds deep relationships in his/her assigned partnership area. They are responsible for proactively understanding and influencing security risk decisions in that area.
- Content Strategist: The Content strategist supports the Product Team in the planning, development, and management of content for each respective product
- Designer: Focused on the look and feel of the product for the enterprise users.
- Product Specialist: Has responsibility for triaging bugs and other issues with each respective product.
- Product Marketing Manager: Has responsibility for the public image of the product and works heavily with the Product Specialist.
- Partner Engineering: Works to integrate each respective product with enterprises by acting as the technical liaison between Meta Engineering and the Enterprises' IT and technical departments.
- Legal: Facilitates enterprise contracts and agreements.
- Security: Responsible for enforcing security and confidentiality standards for each respective product.

In addition to the Security Team and groups outlined above, there are several teams that are key to the ongoing maintenance and support of the main Meta platform and associated control environment.

#### *Meta Enterprise Engineering Team*

Meta's Enterprise Engineering ("EE") Team focuses on corporate IT and is responsible for managing corporate technology assets that support internal company functions.

#### *Meta Global Physical Security Team*

The Meta Global Physical Security Team is responsible for the security and safety of Meta personnel, locations, and brand reputation worldwide. The team is dedicated to taking a progressive and innovative approach to protecting Meta from physical threats.

#### *Meta Infrastructure Team*

The Meta Infrastructure Team is responsible for building and maintaining the systems and facilities on which the Meta site and platform are built and operate.

#### *Community Operations Team*

The Community Operations team is responsible for building and preserving Meta user engagement, including enterprise users, and trust in Meta. Key responsibilities include developing scaled solutions for user issues, analyzing how users interact with products and each other, and delivering qualitative and quantitative insights into user behavior to



the rest of the company. The team also maintains user safety by identifying and resolving instances of abuse, breach of community standards and works to build trust in the Meta experience. The team serves as the voice of the user and works directly with product, engineering, global policy, and other partners responsible for solving these challenges. Community Operations plays an integral role in maintaining and improving the user experience on Meta.

## **Procedures**

### **Security Domains**

Meta designed the Comprehensive Information Security Program (“CISP”) along the security domains (“Security Domain(s)”), each of which includes policies and/or controls that guide Meta’s security practices. The Security Domains cover key components of how Meta protects its Information Systems. Meta considers industry standards when developing and benchmarking the policies and controls in the Security Domains. The Security Domains help Meta implement and maintain a program that is designed to support Meta’s commitment to security, availability, and confidentiality. The Security Domains in the CISP are:

- Application Security
- Asset Management
- Business Continuity and Disaster Recovery
- Change Management
- Configuration Management
- Data Security
- Identity and Access Management
- Logging and Monitoring
- Network Security
- People Security
- Physical and Environmental Security
- Security Incident Response
- Security Compliance, Policy, and Risk
- Third-Party Security
- Vulnerability Management

The sections below describe Meta’s approach to addressing security, availability, and confidentiality for each of these areas.

### **Application Security**

Meta’s Application Security policies and procedures are designed to prevent, detect, and mitigate security vulnerabilities in Meta’s products.





### *Secure Coding*

Meta has secure development and coding processes in place for the design and implementation of code changes. In addition, Meta has developed an expansive set of libraries which automatically implement secure coding standards when they are used by developers.

Meta trains new hires on application security policies and their current roles.

Software engineers receive security training during their orientation (“Bootcamp”), which includes training on common security issues and how to use Meta’s set of libraries and secure application frameworks. Following the Bootcamp, engineers have access to instructional materials on secure coding practices and security-related tools available to them. Continuing security awareness trainings are provided to Meta personnel throughout their employment, such as “Hacktober”, a month-long security awareness campaign that includes security training exercises and security presentations by internal and external speakers.

### *Externally Reported Threats and Vulnerabilities*

Meta has security controls in place to identify bugs and triage, monitor, and mitigate them.

Meta has a Bug Bounty (<https://www.facebook.com/whitehat>) program to facilitate and incentivize the responsible disclosure of bugs that could compromise the integrity of Meta User Data, circumvent the privacy protections of Meta User Data, or enable unauthorized access to a system within the Meta infrastructure. Customers and external users are encouraged to report security and vulnerability issues through the Bug Bounty program. Procedures are communicated to external security researchers through the Meta website. Bug Bounty program submissions are triaged, with validated bugs prioritized and remediated based on assigned severity level. Meta assigns validated submissions made through the Bug Bounty program to the appropriate teams and personnel for triaging, monitoring, and validating. The Bug Bounty program has a Responsible Research and Disclosure Policy in place designed to prevent the premature public disclosure of bugs that could compromise Information Systems and Data.

### **Asset Management**

Meta has tools and processes to track assets in a centralized system (i.e., listing of servers, hostnames, type of devices, hardware type (memory / disk space), location (data center/rack), status (in production/being repaired), etc.).

### **Business Continuity**

Meta has a resiliency program for getting people, teams, and leaders better prepared to effectively respond to and recover from emergency or crisis. The Global Security Resiliency (“GSR”) Team leads company-wide efforts by developing, implementing, and managing programs that enhance our preparedness and capabilities around:

- Business Continuity
- Crisis Management





- Data Center Resiliency
- Resilient Workplace

A Site Resiliency Team has dedicated business continuity resources and has established Business Resiliency Advisory Groups in key business verticals to steer and help evolve Meta's business continuity program.

Each Meta-managed site, office, data center, and region have Site Resiliency Teams to respond to crisis situations. In addition, the Resiliency team develops Site Resiliency Plans to support preparedness and response activities.

Business departments partner with the Resiliency Teams to complete a site/functional Requirements Analysis ("RA", also known as a Business Impact Analysis). The RA assesses teams' functions on its operational, technological, financial, and reputational impacts in a disruption.

The Resiliency Team conducts multiple periodic training and exercises, ranging from geography-specific crisis simulations to preparing data center teams to respond to crisis events and continue operations following a disruption. In addition, teams can conduct their own exercises with guidance from the Global Resiliency Teams.

The Resiliency program focuses heavily on people and processes and supplements Meta's Disaster Recovery efforts that focus on the resiliency of the Company's network, information technology ("IT"), and engineering assets.

Additionally, to limit exposure from a crisis event, Meta writes or replicates data across multiple data center regions for performance and resiliency and automatically routes and load balances network traffic based on latency and network health checks.

Meta has a dedicated team and program to monitor and forecast capacity in order to meet the availability commitments of its products and services.

The team performs Long Range Planning ("LRP"), which involves the forecasting of power, network, and capital expenditures over a period of two to seven years into the future with a goal to also provide forward guidance for the management team to understand upcoming expenses for building out Meta Infrastructure. The LRP process is visited at least on an annual basis and involves multiple teams. The process takes inputs such as:

- Hardware-refresh rate per geographical region
- Organic growth demand for different services
- Estimated timelines for decommissions
- Starting supply, and new supply coming online

Projections are then made to determine if Meta can handle the planned amount of demand based on the current planned supply.



## **Disaster Recovery**

Meta has a dedicated team and redundancy planning for assets to strategize and improve Disaster Recovery (“DR”) capabilities, which makes core infrastructure and software systems resilient to failures ranging from a failure of a single hard disk to the destruction of an entire data center region by a natural disaster.

The DR team provides tools and performs tests to help ensure Meta and its family of applications stay resilient despite site outages.

Disaster Recovery exercises are conducted to verify that Meta can safely and fully disconnect a region with minimal impact to users. Various same day unannounced tests are performed to monitor and learn how products and services react in a catastrophic scenario. Based on the learning, runbooks are updated, and automation opportunities are identified to recover from such scenarios.

## **Change Management**

Meta maintains controls designed to help ensure that changes to code and back-end systems (including infrastructure, back-end environment, and databases) follow approved procedures and are tracked through version control tools. Meta uses a formal process and an internal system to document, track, and review changes. Changes go through the following processes:

### *Change Initiation and Logging*

To initiate a change, developers (“change author”) check out source code (“code”) from a central repository and load it into a testing environment in order to modify the code and test the proposed changes. Once the author of the changes is satisfied with the changes, that author creates a differential record, or ‘diff’, which documents the proposed code changes. Each diff record represents a change to the code base or back-end systems that a developer has proposed for use in production. Each individual diff record documents and tracks the following:

- The delta between the original code and the proposed/changed code,
- The test plans for the proposed change,
- The results of automated testing of the change,
- The peer reviewer for each diff, and
- The peer approval for each diff.

### *Human Code Review and Testing*

After the code is modified by the author in the development environment, it is submitted for peer review. Peer review requires separation of duties; as such, the peer reviewer must be a different person than the change author. After completing the review, the peer reviewer can approve the updated code, or reject the code and request further modifications of the code by the author.



Code changes go through appropriate testing (manual or automated) based on the nature of the proposed changes. The peer reviewer(s) may help determine what testing is appropriate based on the potential risk and impact of the change. Code changes go through automated tools that check for common errors or deviations from best coding practices and for known code patterns that raise security or privacy concerns. These testing tools include features designed to help the author locate the documentation or resources needed to resolve any identified issues. Test types may include:

- End-to-end testing, which may be used depending on the affected library or code path in order to test an entire system, including dependencies,
- Integration testing, which may be used if the change affects separate code paths that work together, to help ensure the change does not negatively affect integration,
- Regression testing, which may be used to help ensure that all relevant tests are triggered following the implementation of a change, or
- Additional use case and functionality-specific tests that may be created by developers and engineering teams to automatically run whenever certain types of changes are initiated.

Testing and approval of the diff are logged by the system to support the code change.

### *Emergency Changes*

In emergency situations, personnel may implement a change without peer review and testing. However, to help ensure that emergency changes are peer reviewed and approved, a retroactive review process is implemented for emergency changes that includes the following steps:

- A task is automatically created and assigned to an infrastructure engineer for triaging the emergency change,
- The change author is required to finish the retroactive review process in ten days,
- The change author must assign the review to an appropriate peer for review and approval, and
- The peer reviewer can approve the change, or mark for further review before approval.

### *Pre-Production Code Push*

Once the code change is approved by a reviewer, the author can commit the code to the central repository. Changes are first made and released to a limited production environment that is only available to Meta personnel, where the changes are tested before being released to the Meta user base. Different application tiers have different push schedules. Changes to source code go through automated tests, which may include linting, static analysis, unit, integration, and end-to-end tests. Developers and engineers build tests to detect code that does not meet Meta's development standards or that causes issues that can be detected in an automated manner.



In order to facilitate the speed and rapid release of code, development and testing is performed on Meta's internal production instances, which also validates that the developed code will work appropriately. Meta has implemented several measures as described below to protect data throughout the development process including:

- Training on Meta's secure coding practices, tools, and all aspects of the technology stack,
- Peer review including review of code, unit testing, and test case development,
- Enforcing strict accountability for changes and their effectiveness during the release process,
- Post-production monitoring including bug bounty and incident management, root cause analysis, and corrective action for identified issues, and
- Development ("dev") servers receive the same level of security configurations across the tech stacks as production systems.

#### *Production Code Push*

Once testing in the Meta Personnel environment is completed, the change is rolled out to a subset of the user base, and then eventually to the entire user base. Meta continues to monitor changes to the code as they are rolled out.

#### *Mobile App Store Releases*

The authorizations to release new versions of mobile code to iOS or Android app stores are strictly limited to a small group of authorized users based on job function. The list of users with authorizations to push Workplace client code to the mobile application stores are subjected to periodic access reviews to validate the appropriateness of active authorizations based on user job duties and employment status. Authorizations are removed for users who no longer require them or terminated.

### **Security Compliance, Policy and Risk**

#### *Compliance*

Meta has established an information security management framework describing the purpose, direction, and principles for maintaining trust. This is accomplished by assessing risks and continually improving the security, confidentiality, integrity, and availability of Meta systems. Meta's security framework is built on the Common Controls Framework ("CCF"). The CCF is a comprehensive set of applicable control requirements that have been rationalized from several different industry information security standards (i.e., ISO/IEC 27001:2013, NIST CSF, SOC 2 trust services criteria, etc.). Meta reviews this framework periodically in order to confirm that management is in alignment with both Meta's business processes and requirements based on internal company feedback, customer requirements, and guidance from industry and regulatory bodies. In addition, Meta conducts regular assessments of compliance with security policies, frameworks, and regulatory requirements.



## *Policy*

Meta maintains a suite of information security policies based on a standard policy framework to enable processes within the policy development lifecycle. The framework provides a structure and parlance for security teams to use in developing and maintaining security guidance, including Policies, Standards, and Guidelines. This framework sets expectations concerning each form of guidance, including how frequently the guidance should be updated, how it should be communicated and enforced, and how exceptions should be handled. Meta also maintains procedures regarding the policy development lifecycle (development, implementation, maintenance, and exception management). Various policies ranging from Information Security Policy, Incident Response, Data Classification, etc. are developed and periodically updated to provide direction for and support the appropriate protection against the unwanted disclosure, modification, or destruction of Meta's data.

## *Risk Assessment and Risk Mitigation*

Management has placed into operation a risk assessment process to identify and manage risks that affect the Company's ability to achieve its defined security, availability, and confidentiality objectives for its platforms.

Meta has further developed a risk management methodology and subsequent procedures to intake, identify, categorize, assess, treat, and monitor security risks. Meta designs, implements, maintains, and documents safeguards designed to protect against internal and external risks identified in risk assessments. Outputs from the risk assessment activities are communicated to relevant management and stakeholders, including the Audit and Risk Oversight Committee. Management is also responsible for implementing appropriate measures to monitor and manage any significant risks identified through this process.

The Security Team relies on inputs from various activities to continually assess and respond to new and changing risks within the environment, including, but not limited to, the following:

- Third-party security assessments
- Penetration testing
- Vulnerability assessments
- Project/system-specific risk assessments
- Bug bounty/white hat assessments

For various internal projects, a dedicated security team member is assigned to work closely with the project team to raise awareness of the risks related to the security, availability, and confidentiality of data. These dedicated stakeholders act as consultants to the engineering and product management teams to support the identification and mitigation of potential threats to Meta's ability to achieve its security, availability, and confidentiality commitments. These security partners support product teams in the investigation of potential risks, assessing the impact of identified risks, establishing



actions to mitigate risks, tracking action to completion through the process, and communication of results of risk assessment procedures.

Additionally, in an effort to promote risk awareness within the Meta environment, the security team encourages management from different departments to report areas where potential vulnerabilities might arise. The team then develops appropriate security exercises that target these areas, with the goal of promoting security awareness to Meta employees.

#### *Security Governance*

Meta has established a security leadership team responsible for the development and implementation of the company's security program. The roles, hierarchy, and responsibilities of the security team, as well as security, availability, and confidentiality policies, are communicated to employees through the internal site that is available to all employees.

#### *Applicable Terms*

Meta communicates its security and confidentiality commitments and obligations to enterprise users, companies, and internal users via the product terms.

#### *System Design Documentation*

Respective product features and system descriptions are communicated to various internal and external stakeholders via posts on websites, blogs, the help center, and materials passed to customers by sales partnership teams.

### **Configuration Management**

Meta uses configuration management tools to manage and monitor the configurations of its systems. The tools automatically push standard policies to servers to help ensure consistency and compliance of the configuration. Alerts are generated and remediation is performed for systems that have not checked in with the configuration management tools. Changes to these configuration systems follow the formal change management process. In addition, access to the configuration management systems is restricted to appropriate individuals based on their job responsibilities.

Configuration management tools are utilized during provisioning to change vendor-supplied default passwords or disable default accounts before a system is deployed.

Additionally, Meta systems are configured to synchronize via Network Time Protocol ("NTP") to redundant stratum GPS coordinated time clocks in Meta data centers.

### **Data Security**

#### *Data and Data Classification*

Meta classifies its data into three main groups: public, internal, and private/confidential:

- Public data is available to the general public and intended for distribution outside of the Company.
- Internal data is only intended for internal use and distribution within the company (i.e. information that the Company has chosen to keep internal).





- Private/confidential data has a reasonable expectation of privacy and/or confidentiality. It is intended for limited audiences, even within the company, and/or is used only for the purposes for which it is collected. For some data types and/or use cases, additional restrictions apply.

Information relating to each respective product is considered private/confidential.

To facilitate deletion, Meta has a data deletion framework that helps ensure user data is deleted appropriately. Deletion scripts are run at a defined frequency to establish timely deletion of data within a reasonable period of time, based on regulatory and compliance requirements. Furthermore, the deletion framework is monitored for issues via “On Call” engineers, and such issues are investigated and tracked through resolution once they are identified. Accounts not deleted in a timely manner are tracked to resolution.

Meta has a “data anonymization” program, which is the process for de-identifying user data in the data warehouse. By default, user data is de-identified. Within 90 days of creation, user data stored within each data warehouse table (i.e., user activity) is either rewritten to remove personal identifiers or replaced with a surrogate. Specifically, each User ID (“UID”) is replaced with a Replacement ID (“RID”). Until a user account is deleted, the UID - RID association remains stored within a secured database. Upon account deletion, the UID and RID association is deleted via the user account deletion process.

#### *Content Delivery Network (“CDN”) Data Encryption*

Cached content on globally distributed content delivery network (“CDN”) infrastructure (i.e., photos, videos, other cached objects, etc.) is encrypted at rest on storage media to reduce the risk of data loss when storage media is moved out of the controlled environment.

#### *Endpoint Security*

By default, Meta uses transport layer security (“TLS”) to encrypt all users’ interactions with Meta and each respective product irrespective of whether these interactions are made via a browser or the application programming interface (“API”). The digital certificates, used to provide the TLS encrypted connection between Meta and the enterprise user’s browser, are from a trusted Certificate Authority, and are current (i.e., the certificate is valid and has not expired).

Meta laptops are protected via full disk encryption and anti-malware solutions. Laptops are kept in compliance with Meta’s security configuration standards using centralized management tools that are also used to deploy patches and updates. Additionally, Meta provides employees with details of the status of their device’s compliance with corporate security policies through a personalized portal. The portal provides details of the status of device management, software updates, disk encryption, and potential vulnerabilities.

## **Identity and Access Management**

#### *Logical Access for Meta Personnel*

Upon joining Meta, personnel (employees and contingent workers) requiring logical access to internal systems are provisioned with access based on job function and/or



business needs. There is an automated process to retrieve new employee information from Meta's Human Resources ("HR") system to create associated Active Directory and Lightweight Directory Access Protocol ("LDAP") Unix accounts in the system. This corporate Unix account is used for internal tool authentication, as well as to access the third-party applications through a single-sign-on mechanism. The access to create a production Unix account is manually submitted by the user, which is then approved by the requestor's manager or supervisor. Access to development servers ("dev servers") is authenticated via the production Unix account only and authorized via the system using two factors: a certificate and a separate authentication token (either user confirmation using a mobile phone or via a one-time password). Only those users who explicitly request access for production Unix accounts are granted unique credentials to access development servers; corporate Unix accounts cannot be used to access the development servers.

From dev servers, authorized users can access production servers via Secure Shell ("SSH") using a certificate issued on the dev server. Authorized users can generate a certificate from the Meta Certificate Authority ("CA"), which expires in a pre-defined time based on their job role or pre-approval.

Access to internal tools and data stores storing product specific data is restricted to specific authorized groups, users, and services. Only authorized maintainers, and the members of the Security Operations team, can add new users to these groups and/or services upon the request submitted by the user via permission request form. Based on the specific group's configuration, the request is routed to the appropriate individual for manual approval. In addition, group membership and Access Control List ("ACL") configurations to product-related access groups are reviewed on a quarterly basis for appropriateness.

When not connected to Meta's corporate network, remote access is provided via a TLS-encrypted Virtual Private Network ("VPN") or from a managed device through managed gateways that requires two-factor authentication. Meta also encrypts sensitive network traffic between data centers and uses key-based encryption to protect sensitive data.

When personnel are terminated, there is an automated process to pick up the termination date in the HR system, which enables the Identity Management system to schedule the disable date for the users' Active Directory, UNIX, LDAP, and other internal accounts.

Passwords for Active Directory and UNIX systems are configured to comply with the Company password policy.

#### *Logical Access for Company Admins and Users*

After initial setup, Meta transfers ownership of the private community to the company. As part of the initial provisioning process, Meta will provision at least one company user with administrator privileges. From there, the company administrators are responsible for the provisioning and deprovisioning of additional company users, managing groups, managing content, and configuration of community settings. Companies have the option to enable Security Assertion Markup Language ("SAML") capable identity systems managed by the company to authenticate company users and enable single sign-on ("SSO") with Workplace from Meta.





Companies will need to assign administrators within the Device Manager portal for administering and configuring the environment.

On a need-to-know basis, engineers and teams supporting Workplace products may access Workplace data (i.e., for resolving a support ticket raised by the customer). Access to customer data is logged, closely monitored and any suspicious behavior is thoroughly investigated as described in the Incident Management section. Meta has a zero-tolerance approach to abuse, and improper behavior results in termination.

### **Logging and Monitoring**

Meta's Logging and Monitoring policies and procedures are designed to help ensure that logs are effectively generated and reviewed to support the detection and investigation of suspicious events in production and corporate systems.

Meta's internally built intrusion detection system is used to collect and monitor logs from production and corporate systems. Meta also utilizes endpoint-monitoring software to log and monitor activity on Meta-managed IT assets. Security logs are preserved using both proprietary and third-party tools.

The monitoring of system configurations and security settings is managed by configuration management tools. These tools continually update security settings and configurations on production servers with master settings to help ensure systems are consistent with expected security standards.

Meta performs security event logging and monitors for threats in accordance with predefined security criteria configured in a centralized security monitoring tool. Alerts are reviewed by authorized personnel.

Furthermore, Meta has Distributed Denial-of-Service ("DDoS") detection and mitigation mechanisms in place to protect the network from denial-of-service attacks. In addition to redundancy built into the edge network, Meta uses a cutting-edge Berkeley Packet Filter ("BPF") based DDoS mitigation capability facilitated by Droplet. Droplet is a generic framework to write BPF policies to drop packets at the earliest stage in the networking stack, preferably at line rate. It was born as an anti-DDoS measure and is the preferred place to plug in customized BPF code for packet drops.

### **Network Security**

Network traffic to and from untrusted networks passes through a network device that filters traffic in accordance with identified security requirements and business justifications.

### **People Security**

Meta's mission is to give people power to build community and bring the world closer together. Meta HR helps drive that mission through finding, growing, and retaining the best people who are committed to that mission. Aligned with Meta's focus on protecting its users from all manner of threats, HR understands that this starts with the people that Meta hires. Job requisitions for available jobs at the Company have written job profile descriptions which outline the responsibilities of the position and required qualifications/experience.



Subject to applicable law and regulations, Meta employees and contingent workers are required to complete background checks during their onboarding process. Meta monitors and reviews progress reports to help ensure completion of background checks prior to being granted access to Meta worksites and information systems, including Meta-issued devices or physical access tokens (i.e., ID badges, hardware-based multi-factor authentication tokens, etc.). If Meta identifies a candidate who has not completed the background checks, the notification and escalation procedures are enforced in accordance with the Meta Background Check Policy.

Meta employees and contingent workers are required to sign a confidentiality statement upon hire agreeing to the terms set forth in Meta's Confidentiality Information Agreement, which includes information regarding disciplinary actions for non-compliance. Additionally, employees are shown the security policies and procedures as part of the onboarding process.

Finally, Meta employees and contingent workers are encouraged to report known and suspected violations of (a) laws, governmental rules, and regulations, (b) accounting, internal accounting controls and auditing matters, or (c) Meta's Code of Conduct or other policies to their managers or managers in the Legal, HR, or Internal Audit teams. Management provides the Audit and Risk Oversight Committee with regular reports regarding significant complaints, including those involving auditing or financial reporting. These reports include the status of the investigation and the dispensation of the complaint.

### *Electronic Communications*

Meta maintains policies for the appropriate use of electronic communications by Meta personnel. These policies set restrictions regarding the content of messages sent by Meta personnel, disclosure of privileged communications, endorsements, public representations, spam, and intellectual property. These policies also advise employees of Meta's right to collect and review electronic communications for security and investigation purposes.

### *Training and Awareness*

Depending on roles and responsibilities, there are various trainings available to Meta employees and contingent workers.

#### *Privacy and Security Awareness Training*

New and existing Meta employees and contingent workers are required to complete a computer-based training focusing on confidentiality and security within 30 days of hire. Topics covered include Meta's key privacy principles, Meta's policies, privacy laws and regulations, vendor security audits, privacy and security by design, the importance of ensuring user data is kept secure from unauthorized access, and general security awareness leading practices. The Security Awareness Training Program performs weekly monitoring to help ensure employees receive and take their mandatory training. The Security Awareness Training Program enforces notification and escalation procedures for participants identified as not having completed training assignments.



Meta's Security Team conducts an annual, month-long security awareness campaign called "Hacktober". The campaign includes numerous types of hacks, where the Security Team targets Meta employees and vice versa. Other activities include security scavenger hunts that look for bugs in code, presentations from internal and external speakers, and an internal security capture the flag.

Additionally, Meta's security team has regular all-hands meetings. During the meetings, security topics are communicated to the team, such as the introduction of new security tools and common threats or security issues that Meta is facing. Meta also encourages security team members to attend security conferences hosted outside of the Company to increase awareness of environmental, regulatory, and technological changes that may impact system security and confidentiality.

### *Engineering Bootcamp*

Some teams such as engineering, sales, and user operations have specific onboarding training programs for new hires. For engineers and product managers, there is a four to six-week program called "Bootcamp", which includes all-day classes, assignment of coding tasks, mentoring sessions, and training on common security issues in code.

The goal of Bootcamp is to train new engineers and product managers on Meta standards and practices, and to develop their technical skills so that they have the right resources to fulfill their responsibilities (including different training tracks available during the onboarding process). These options provide individuals with general training, as well as role-specific trainings necessary to understand the Meta environment. These trainings include guidelines on Meta's secure and quality development procedures, tools, and other resources used in the development, testing, and monitoring process. Trainings including the following focus areas:

- Backend/Systems
- Web
- iOS
- Android
- Machine Learning

## **Physical and Environmental Security**

### *Physical Access to Meta Premises and Data Centers*

Physical access restrictions are implemented and administered so that only authorized individuals have the ability to access Meta facilities. Meta either owns or leases and operates data center facilities in the following geographical regions:

- North America
  - Altoona, Iowa
  - Ashburn, Virginia
  - Eagle Mountain, Utah



- Forest City, North Carolina
- Fort Worth, Texas
- Henrico, Virginia
- Huntsville, Alabama
- Los Lunas, New Mexico
- New Albany, Ohio
- Newton County, Georgia
- Papillon, Nebraska
- Prineville, Oregon
- Santa Clara, California
- Europe
  - Clonee, Ireland
  - Odense, Denmark

Access to Meta facilities is restricted through badge access, monitoring through the use of closed-circuit television (“CCTV”) cameras and by guard staff 24 hours a day, 7 days a week. On-premises guard staff are responsible for monitoring facilities and responding to physical security alerts. Physical access restrictions are implemented and administered so that only authorized individuals can access Meta facilities. Meta premises are controlled through badges issued to Meta personnel (including employees, interns, contingent workers, and vendors). Internal resources are provided to support compliance with badge access policies, and Meta maintains a dedicated mechanism to troubleshoot issues related to badge access. Where higher security is required based on increased risk, badge access privileges are limited to employees on a need-to-access basis. Access to higher risk areas is monitored through enhanced physical and electronic means. Meta uses a combination of owned and leased third-party data centers to support its products. Owned and third-party data center locations employ badge readers and/or biometric fingerprint devices.

All visitors must register with Meta, present a valid ID, and sign a non-disclosure agreement, or otherwise obtain an approved exception. Visitors must be escorted while on premises at all times. Visitors must also visibly wear a visitor lanyard at all times and return the lanyard before leaving Meta premises.

Meta policies require pre-approval for access to data centers and server rooms. In addition to badge readers, data center locations may also employ additional security measures, including biometric fingerprint devices and motion sensors. Access to the owned data centers is reviewed on a quarterly basis for appropriateness. For third-party data centers, access is reviewed on a monthly basis for appropriateness. Additionally, Meta has onsite data center managers who conduct monthly facility access reviews and review the data center leasing companies’ applicable audit reports. These processes provide a mechanism to safeguard and restrict access to Meta cages and suites in third-



party data centers through appropriate authorization, and that the controls implemented are designed and operating effectively, and data centers meet Meta security, availability, and confidentiality commitments.

Meta conducts security assessments of the third-party data centers before the sites go live. Meta's security compliance team validates the site security requirements are implemented according to the applicable security, regulatory, and compliance standards. This is to help ensure that any third-party data center does not receive production traffic unless it meets Meta security and availability expectations.

In addition to maintaining strong physical security standards at owned locations, Meta also maintains strong security at the leased locations by annually reviewing data center reports around security, confidentiality, and availability commitments.

#### *Data Center Environmental Security*

At Meta-owned data center locations, temperature and humidity levels are maintained and monitored at appropriate levels. Meta also has appropriate fire detection and suppression equipment in place at data centers and in-scope co-locations that meet local legal and regulatory requirements. Meta-owned data center facilities have adequate redundant secondary power (UPS/CPS), backup generator units, and telecommunications to support critical systems in the event of a utility outage. For leased data centers, Meta relies on the vendor for appropriate data center environmental security controls and reviews their SOC 2 report on an annual basis.

#### *Data Disposal*

Meta has a process in place for the secure destruction of decommissioned electronic media containing Workplace product data. This includes wiping or physical destruction. Destruction activities are logged and where destruction is conducted by a third party, a "certificate of destruction" is also issued by the vendor and retained by Meta. Electronic media does not leave Meta's chain of custody without documented proof of wiping or physical destruction.

### **Security Incident Response**

Incidents relating to site, platform, or infrastructure issues are managed and escalated through the general incident management process. Incidents are tracked in the Meta incident management system and assigned a severity level. The Incident On-Call team will evaluate each incident ticket in the Meta incident management system to determine the severity level (which impacts the resolution timing) is appropriate. Policies and procedures for handling security and privacy incidents are documented and published internally.

#### *Incident Response Procedures*

Meta has security tools in place to prevent and detect unauthorized access by internal and external users. Meta implements rules that trigger alerts when abuse or security events are detected. When alerts are triggered by either automated, user, or employee reported means, Meta follows a defined process to respond and mitigate the threat.



## *Security Incident Reporting and Resolution*

Meta has dedicated teams for handling a variety of security incidents including, but not limited to, incidents involving external threat actors, internal threat actors, lost or stolen devices, service disruptions, incidents involving regulated data, and incidents requiring coordination with law enforcement.

- **Internal Detection & Response (“IDR”):** Responsible for the management of security incidents related to employees, contractors, and external threats. The IDR Team has the authority to investigate cases of internal abuse and insider threats, which may also lead to the collection of evidence of employee activity on corporate networks or devices.
- **Global Legal Privacy Incident Management (“GLPIM”):** Responsible for the legal analysis to determine notification requirements to regulators and/or impacted data subject(s), and where applicable, to communicate with relevant regulatory authorities.
- **Cybersecurity Law & Investigations:** Responsible for investigating information security incidents. Manages engagement with Outreach Team, decisions to make law enforcement referrals, and information sharing with other entities.

The designated teams, as described above, monitor and resolve security incidents based on company policies and help ensure that appropriate action is taken in a timely manner.

Internal security incidents are tracked in tools that are only accessible to a limited number of users, primarily within the Security Team. The Company uses these tools to identify violations based on predefined security rules.

Meta maintains an Incident Management Framework (“IMF”), which outlines the framework to assess and respond to data incidents and facilitate data subject protection and notification in case of incidents.

Once an incident has been declared that requires external communication, the GLPIM team members perform a risk assessment and analysis to assess potential risk to data subjects and requirements for regulatory notification are determined.

In addition to the security incident management process, the Company also has a formal process for identifying security threats through periodic vulnerabilities and penetration testing.

## **Third Party Security**

### *Third Party Security Program*

Any third party that is sharing or receiving personal information or sensitive confidential business information; collecting, storing or processing Meta data; integrating with Meta systems; accessing Meta systems and networks; or performing a service on behalf of Meta or attributable to Meta (i.e., Microsite) must submit to a third-party assessment and agree to appropriate contractual provisions prior to them being retained. Third party assessments are conducted by Meta security personnel and are based on a range of factors. The level of assessment conducted for each third party is determined according to the type of data the third party may process and the engagement use case.





### *Third Party Assessments*

Meta has implemented controls with respect to third parties, including implementing policies and standards to select and retain third parties capable of appropriately protecting the security and confidentiality of user data received from Meta.

Meta's security team has a process for conducting due diligence on third parties who may receive user data in order to evaluate whether their data security standards are aligned with Meta's commitments to protect user data. As part of the due diligence process, Meta asks prospective third parties to complete a Third-Party Security and Privacy questionnaire to assess whether the third party meets Meta's functional security requirements to protect the privacy and confidentiality of user data. The questionnaire is targeted to obtain the following information about a third party prior to onboarding:

- Type of service provided by the third party and specific use case for the engagement
- Where and how the third-party stores data
- What types of data the third party collects and how this data is being collected
- Information about the third party's security and privacy frameworks

Based upon the third party's responses, third parties are classified as Lower, Medium, Higher, or Escalated Risk, which, in turn, determines the approval status as Approved (Low, Medium, or High Risk), or Escalated (Escalated Risk). If the Meta security team gives an Escalated risk rating to a third party, the decision whether to continue onboarding the Third Party is escalated to Legal and Business teams.

For use cases involving solutions residing in Meta infrastructure, integration with Meta systems, or third parties developing a consumer/external facing website for Meta, Meta will conduct an additional in-depth technical review following the completion of a Third-Party Assessment. The technical review seeks to address the risks posed to Meta's environment, beyond the scope of the Third-Party Assessment.

Meta also has a contract policy (the "Contract Policy"), which governs the review, approval, and execution of contracts for Meta. Meta's pre-approved contract templates require third parties to implement and maintain appropriate protections for user data. Meta reviews contracts that deviate from the pre-approved templates to help ensure that contracts with applicable third parties contain the required privacy and confidentiality protections. Meta Legal documents review of any such contracts through formal approval prior to contract execution.

### *Software-as-a-Service*

Meta policies govern the use of Software-as-a-Service ("SaaS") solutions to receive, transmit, store, and process Meta's data. New SaaS solutions that have not previously been subject to a Third-Party Assessment must complete an assessment.



## **Vulnerability Management**

Meta has a Vulnerability Management Team in place that is responsible for performing vulnerability scans/detection to identify and evaluate the risks posed by vulnerabilities. The Vulnerability Management Team also works on identifying and prioritizing threats posed, associating threats with owners, and working towards an acceptable remediation of the threat or acceptance of risk. External scanning is performed periodically for scoped systems, and internal scanning and detection is performed on a continuous basis. The results are validated internally and tracked to resolution.

Penetration testing is performed as needed by designated security engineers or external service providers who specialize in attack and penetration testing. Malware defense solutions that detect intrusion or infection are implemented on endpoint devices. Additionally, as the environment is managed by a configuration management tool, once an identified vulnerability is remediated, the corrective action or relevant update is pushed out to all in-scope devices.

## **Impact of Covid-19 (Coronavirus)**

In response to the global Covid-19 pandemic and at the direction of local, state and federal / governmental authorities in the jurisdictions in which we operate, Meta implemented a work from home policy as of March 2020 for all non-essential employees and vendors. The architecture of our platforms and product has been designed in a manner which enables us to continue business as usual operations irrespective of the physical location of our employees. Meta data centers continue to operate as normal.





## Complementary User Entity Control Considerations

The Workplace from Meta Product was designed with the assumption that certain controls are in operation at user entities of this report (i.e., developers using the Product). This section describes those controls that should be in operation at the user entity to complement the controls within the Workplace from Meta Product. In certain situations, the implementation of specific controls by the user entity is necessary to achieve certain service commitments and system requirements based on the applicable trust services criteria included in this report.

The user entity should evaluate its own internal control structure to determine if the appropriate controls are in place. Examples of controls that should be implemented to user entities in order to rely on this report include, but are not limited to, the following.

| Complementary User Entity Controls (“CUEC”)   | Related Criteria        |
|---|-------------------------|
| <ul style="list-style-type: none"><li>• CUEC 1 – User entities are responsible for maintaining appropriate documentation supporting the appropriate use of Workplace from Meta, as needed by their users, administrators, and auditors.</li></ul> | CC2.3                   |
| <ul style="list-style-type: none"><li>• CUEC 2 - User entities are responsible for managing access configurations within Workplace from Meta to appropriately assign access to their users.</li></ul>   | CC6.1<br>CC6.2<br>CC6.3 |
| <ul style="list-style-type: none"><li>• CUEC 3 - User entities should establish, monitor and maintain sufficient internal controls to help ensure appropriateness of access to their Workplace Instances.</li></ul>                               | CC6.2<br>CC6.3          |
| <ul style="list-style-type: none"><li>• CUEC 4 - User entities should disable a User’s ID and credentials immediately upon a user’s termination and end any active sessions for the user.</li></ul>   | CC6.2<br>CC6.3          |
| <ul style="list-style-type: none"><li>• CUEC 5 - User entities should review security access and authorization limits on a periodic basis and monitor all user access and authorization limits.</li></ul>   | CC6.2<br>CC6.3          |
| <ul style="list-style-type: none"><li>• CUEC 6 - User entities are responsible for timely notification to Meta of changes to authorized administrators on their enterprise account.</li></ul>   | CC6.1<br>CC6.2<br>CC6.3 |
| <ul style="list-style-type: none"><li>• CUEC 7 - User entities are responsible for securely implementing and maintaining effective internal controls over any single sign-on solution if used in conjunction with Workplace from Meta.</li></ul>  | CC6.1                   |



| Complementary User Entity Controls (“CUEC”)  | Related Criteria |
|--|------------------|
| <ul style="list-style-type: none"><li>• CUEC 8 - User entities are responsible for the secure handling and storage of any administrative access tokens generated for use with relevant Workplace from Meta APIs.</li></ul>   | CC6.1            |
| <ul style="list-style-type: none"><li>• CUEC 9 - User entities are responsible for ensuring physical access controls are in place to protect their machines accessing Workplace from Meta.</li></ul>   | CC6.4            |
| <ul style="list-style-type: none"><li>• CUEC 10 - User entities are responsible for staying informed of new features and functionality by reviewing Workplace service update bulletins and release notes. User entities are responsible for updating any internal controls or processes, which may be impacted by the feature change or new functionality.</li></ul> | CC2.3            |
| <ul style="list-style-type: none"><li>• CUEC 11 - User entities are responsible for communicating any bugs or processing issues discovered to Meta.</li></ul>  | CC7.1<br>CC7.2   |
| <ul style="list-style-type: none"><li>• CUEC 12 – User entities are responsible for requesting data deletion in line with their requirements.</li></ul>  | C1.1<br>C1.2     |
| <ul style="list-style-type: none"><li>• CUEC 13 - Meta does not provide an archiving service, and user entities are solely responsible for creating backups of their Data.</li></ul>   | C1.1<br>C1.2     |

The list of complementary user entity control considerations presented above does not represent a comprehensive set of all the controls that should be employed by the user entity. Other controls may be required at the user entity.

---

## **Attachment B – Principal Service Commitments and System Requirements**

---



## Principal Service Commitments and System Requirements

Meta designs its processes and procedures to meet its objectives and commitments. Those objectives are based on the service commitments that Meta makes to user entities, the laws and regulations that govern the provisioning of the company's products, and the operational and compliance requirements that Meta has established for its services.

Security, availability, and confidentiality commitments to user entities are documented and communicated in the Meta policies and terms governing Workplace are available [online](#).

These commitments are standardized and designed to meet the requirements for a broad set of user entities. The commitments include, but are not limited to, maintaining appropriate technical, organizational and security measures designed to protect against the accidental or unauthorized access, use, alteration, disclosure, or destruction of data within Meta systems. Support request initial response times are based on Workplace plan.

Meta establishes operational requirements that support the achievement of security, availability, and confidentiality commitments and compliance with relevant laws and regulations, and other system requirements. These requirements are communicated in Meta's publicly available policies and terms [online](#). Information security policies define an organization-wide approach to how systems and data are protected. These include standards and practices around how the products are designed and developed, how the products are operated, how the internal business systems and networks are managed, and how employees are hired and trained.

Meta products are designed based on the assumption of a shared responsibility model as it relates to the design, implementation and operation of controls. As part of this model, both Meta and user entities are responsible for aspects of the security, availability and confidentiality posture of the products. Details of the responsibilities of user entities can be found in the terms and policies on the Meta's website and in the complementary user entity controls (CUEC) section of the SOC 3 report.

---

**Attachment C – Workplace from Meta, General Data  
Protection Regulation (“GDPR”), Security  
Notifications, and Data Transfer**

---



## **Workplace from Meta, General Data Protection Regulation (“GDPR”), Security Notifications, and Data Transfer**

Since its implementation on May 25, 2018, the GDPR has sought to harmonize and clarify EU data protection law, whilst also imposing certain new requirements. Many of the GDPR’s requirements fall on data controllers. This is the organization or party that decides the ‘purposes’ and ‘means’ of any processing of personal data.

Workplace customers are the data controller in respect to the handling of personal data processed within their Workplace instance and the Workplace Agreement imposes various data processing obligations onto Meta, as data processor of customers, including in the Data Processing Addendum to the Workplace Agreement.

For more information see:

- <http://www.workplace.com/workplace/blog/workplace-and-gdpr>
- <https://www.workplace.com/datatransfers>
- <https://www.workplace.com/subprocessors>

### *Safeguards and Contractual Commitments*

GDPR requires data controllers to engage data processors with appropriate safeguards, in order to help ensure an appropriate level of protection for personal data.

Our product, privacy and engineering teams work closely to make sure Workplace complies with the GDPR and enables our customers to comply with their obligations under the GDPR.

Prior to 25 May 2018, we updated our Workplace agreements to provide our customers with the contractual commitments which they require from their data processors under the GDPR.

In particular, we included a new Data Processing Addendum in the Workplace agreement, to address the requirements of Article 28 GDPR.

For data transfers outside of the EEA, the Workplace Agreement also contains the Workplace European Data Transfer Addendum, pursuant to which Meta transfers data under the new Standard Contractual Clauses, specifically module 3 (processor to processor), as approved by the recent European Commission decision 2021/914.

### ***Data Security***

GDPR requires Workplace customers to engage data processors who can provide an appropriate level of security to meet the requirements set out in the new regulations. The safety of the personal data we process for our customers is of the utmost importance to us.



We undergo regular security audits and Workplace is ISO27001 certified and has implemented leading practices per ISO27018. These latest certificates can be viewed by visiting [workplace.com](https://workplace.com).

Our Workplace Agreement also makes commitments on security, with the Data Security Addendum providing contractual commitments on top of the security measures we already have in place.