@workplace

from FACEBOOK

System and Organization Controls (SOC) 3 Report

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

For the period January 1, 2020 through December 31, 2020

Workplace from Facebook Product

TABLE OF CONTENTS

Section I – Report of Independent Accountants

Report of Independent Accountants

To the Management of Facebook, 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 Workplace from Facebook Product Based on the Trust Services Criteria for Security, Availability, and Confidentiality" (Assertion), that Facebook's controls over the Workplace from Facebook Product (System) were effective throughout the period of January 1, 2020 to December 31, 2020, 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

Facebook'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 System and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our 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 requirement

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 Facebook'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 Facebook'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 Facebook Product" (Description) indicates Facebook'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 Facebook'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 Facebook Product and General Data Protection Regulation (GDPR)" is presented by management of Facebook 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 Facebook'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, Facebook's controls over the system were effective throughout the period of January 1, 2020 to December 31, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted use

This report is intended solely for the information and use of Facebook and Facebook customers of the Workplace from Facebook Product and is not intended to be, and should not be, used by anyone other than these specified parties.

April XX, 2021

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

1

FACEBOOK Hacker Way

Menlo Park, California 94025
United States of America

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

We, as management of, Facebook, Inc. are responsible for:

- Identifying the Workplace from Facebook 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 requirement
- 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, 2020 to December 31, 2020, 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,

Facebook Management

Attachment A – Workplace from Facebook Product

Scope and Purpose

This System and Organization Controls ("SOC") 3 report is an examination of the internal controls of Facebook Inc.'s. (herein referred to as "Facebook", "the Company" or "Management") Workplace from Facebook Product relevant to the security, availability and confidentiality trust services criteria as set forth in TSP section 100 of the 2017 Trust Services Principles and 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.

This section of the report was prepared by the management of Facebook 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 and is intended to provide user organizations with information about the Workplace from Facebook 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, 2020 to December 31, 2020. It does not and is not intended to encompass all aspects of the services, procedures, or controls performed by Facebook, Inc.

Company and Business Overview

Facebook is a publicly traded U.S. company headquartered in Menlo Park, California, with approximately 139,000 employees as of February 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 Facebook 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 Facebook Platform to build applications (apps) and websites that integrate with Facebook to reach its global network of Facebook users and to build products and services that are more personalized, social, and engaging.

Workplace from Facebook Product Overview

Background

Workplace from Facebook 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 Facebook's infrastructure, but it is a separate platform. Workplace is similar to the public-facing products but allows an enterprise to establish and manage their own individual instance of Facebook. 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.

Facebook offers three plans of the Workplace product; Essential, Advanced and Enterprise.

Note: The Workplace Essential tier will be sunset on February 10, 2021 see link.

Unless otherwise noted, references to “Workplace” in this report refer collectively to Workplace Essential, Advanced, and Enterprise. In addition, the scope of this report and the controls described herein are applicable to all Workplace plans unless denoted otherwise.

Development and Management

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

- Access to data is controlled based on the agreements that Facebook 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 Facebook” 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 Facebook which is driven by the dedicated Facebook Security team and sponsored by the Company’s senior leadership.

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

Technology Stack

Infrastructure

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

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

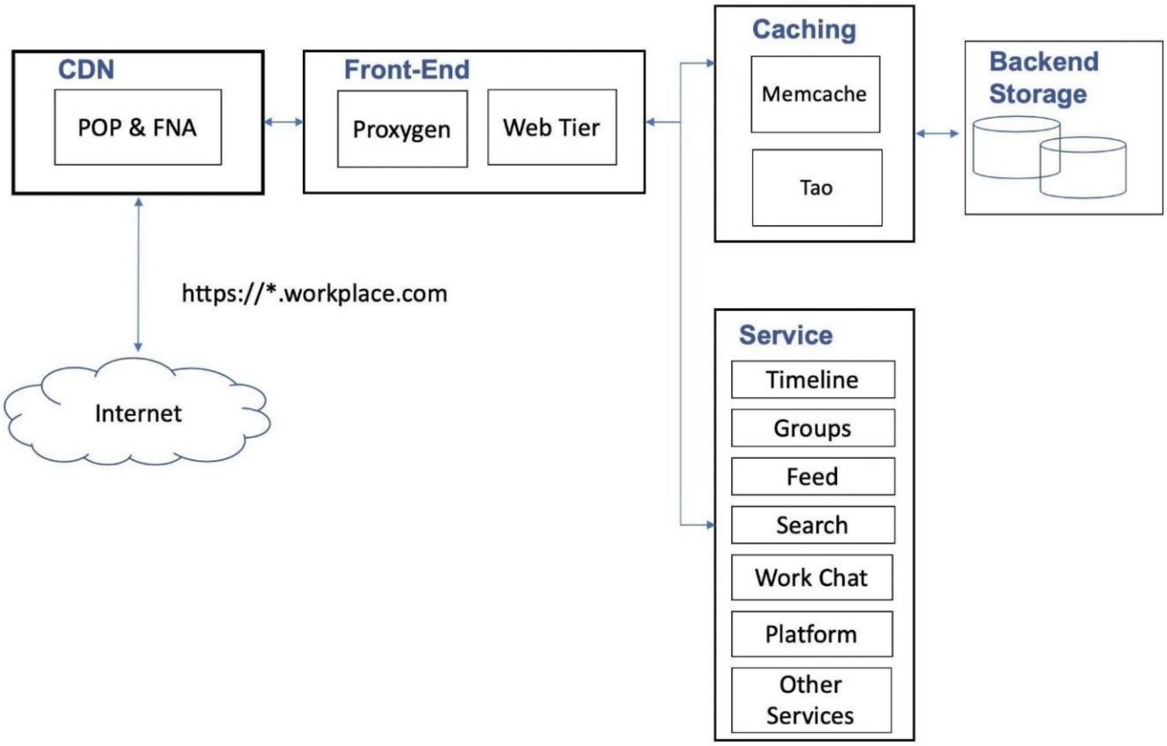

Figure 1: Workplace from Facebook Components

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 Facebook’s web (www) environment. Within this environment, “Workplace from Facebook” data is stored on the same servers used to store data originating from Facebook’s www platform, and thus, inherits the same security controls. To further protect the data of organizations using “Workplace from Facebook”, Facebook segments

“Workplace from Facebook” data through the strict security controls described in the Managed Communities section below.

CDN

Internet to Facebook traffic is mainly comprised of two types of requests: dynamic (e.g. requests for Messages (delta), Timeline, Feed, Groups, Search, or other services) and static requests (e.g. requests for images, videos, or other static content). To handle the large volume of requests and ensure a performant experience for users, Workplace uses a Facebook owned and operated Content Distribution Network (CDN). This CDN includes several layers of cache including FB Edge Point of Presence (PoP) and Facebook Network Appliances (FNA - FB owned and protected network appliance deployed at ISPs). 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 Facebook equipment to either fulfill the request itself or direct the request to the closest Facebook data center to retrieve the specific services and content.

Front-End

Facebook’s front-end is responsible for receiving and responding to requests made by enterprise users by way of the CDN and Facebook datacenter Proxygen servers. Running Hip Hop Virtual Machines (HHVM), Facebook’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 (e.g. Timeline, Feed, Groups, and Search) when an enterprise user requests them.

Caching

To reduce latency and retrieval times, “Workplace from Facebook” 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.

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 (e.g. 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 Facebook" leverages Facebook'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 www interface (https://company.workplace.com), the mobile site (https://company.m.workplace.com), or the "Workplace from Facebook" 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. www
2. Mobile Apps
3. Company dashboard
4. Workplace from Facebook Account Management Application Programming Interfaces (APIs)
5. Workplace from Facebook Product (Integrations)

Enterprise 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 Facebook 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 of the Workplace features and functionality through their mobile devices. The mobile applications connect to the Workplace infrastructure described above over an encrypted API connection. Similarly, desktop workplace chat for windows and Mac and portal from Facebook are available.

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 Facebook 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 Facebook Account Management API* is a System for Cross-domain Identity Management (SCIM) which allows enterprise administrators to manage enterprise users including creation of users, user groups, and removal of users adhering to the SCIM standard.
- *Workplace from Facebook Graph API* allows enterprise 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. Our industry standard APIs allow for real-time activity monitoring and content exports.

Platform

The Workplace Product provides company admins an ability to integrate and configure third party applications with their 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 Facebook
- Third-Party - built by a (verified) partner
- Custom Integrations - built / operated by the customer. Not available for Essential Tier

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 SaaS and 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 an enterprise signs up for Workplace, Facebook creates an enterprise 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 Facebook account. These boundaries restrict the ability to access and view content to only those enterprise users that belong to the instance; thus, no content is publicly accessible. The enterprise 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, Facebook utilizes their Entity (ent) framework. These ents act as objects that allow “Workplace from Facebook” data to be organized by instance. In addition, when an enterprise user has a relationship with an object (creates a post, likes an object, etc.), an assoc or link is created between the enterprise user and the activity/object. Assocs are also utilized to ensure that relevant content for each enterprise is displayed appropriately, limiting viewing rights to those enterprise users that belong to the instance, or within the ents boundaries and assocs.

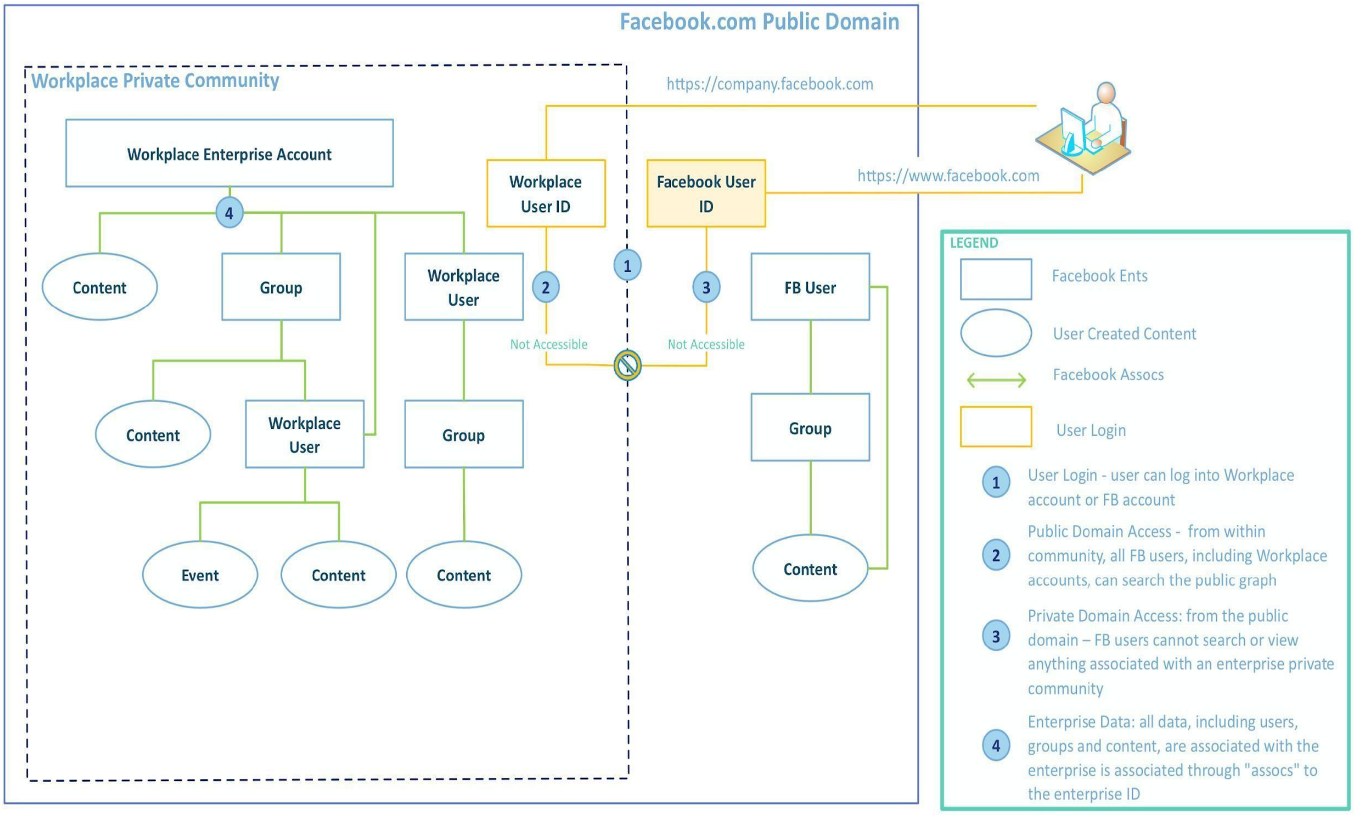
Facebook.com Public Domain
Workplace Private Community
https://company.facebook.com
https://www.facebook.com
Workplace Enterprise Account
Workplace User ID
Facebook User ID
4
1
2
3
Content
Group
Workplace User
FB User
Not Accessible
Not Accessible
Content
Workplace User
Group
Group
Event
Content
Content
Content
LEGEND
Facebook Ents
User Created Content
Facebook Assocs
User Login
1 User Login - user can log into Workplace account or FB account
2 Public Domain Access - from within community, all FB users, including Workplace accounts, can search the public graph
3 Private Domain Access: from the public domain – FB users cannot search or view anything associated with an enterprise private community
4 Enterprise Data: all data, including users, groups and content, are associated with the enterprise is associated through "assocs" to the enterprise ID

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 on-boarded.

During initial company instance setup, Facebook account managers may provision an initial set of company users, including assigning at least one administrator profile to the company workplace instance. After initial setup, Workplace transfers ownership of the instance to the enterprise.

Company administrators can utilize the SCIM standard and 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 Facebook”.

Workplace is built to provide everyone in an organization a voice, whether they work in the head office or on the factory floor. Facebook recognizes 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 access codes. With these access codes, employees can activate their account without having a corporate email address. Enterprises can enable better frontline user management and experience using frontline add-on.

Once a new Workplace profile is set up, an employee will receive an email inviting them to activate the respective "Workplace from Facebook" profile. Enterprise user Workplace profiles are not linked to or associated with an individual's personal Facebook account.

End User Management

Once an instance has been created by Facebook, enterprise administrators are responsible for performing all management functions of the Workplace community. Enterprise administrators are expected to manage enterprise user-generated content, provision and deprovision enterprise 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 times are 4 hours for Enterprise customers and 24 hours for Advanced from the time an email confirmation is received that a support ticket is raised. Workplace Essential does not include a Direct Support Channel.

Data Management

The data gathered from Workplace will be gathered on behalf of the enterprise signed up to use Workplace as a service. Enterprise user-generated content contained within the enterprise's instance, as well as logged enterprise user activity is stored on Facebook's servers until the end of the Workplace service contract or until the enterprise decides to delete the data. Facebook does not provide an archiving service, and the customer is solely responsible for creating backups of their Data. Customers may delete user content at any time during the term through the system administrator functionality of Workplace, including their own instance.

Enterprise admins may delete groups or enterprise user-generated content. Once the option to delete the data is confirmed, the data is deleted in alignment with Facebook's data deletion policies. Enterprises also have the option and ability to access, correct, backup or delete any relevant data via the "Workplace from Facebook" API. Further, enterprise data is not collected or utilized for the purposes of advertising by Facebook.

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

Facebook 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 Facebook's unique Information Systems and business needs, including safeguards appropriate to Facebook's size and complexity, the nature and scope of Facebook's activities, and the sensitivity of the user information Facebook processes and stores.

Comprehensive Information Security Program

Roles and Responsibilities

Facebook 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. Facebook's security efforts are overseen by the Security Team, which has the primary responsibility to implement and maintain Facebook'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 Facebook's Information Systems;
- **Detection and response**, tracking, analyzing, and monitoring risks to Facebook's Information Systems;
- **Measurement and validation**, evaluating the effectiveness of Facebook's security safeguards; and
- **Programs and operations**, supporting the delivery and enhancing the effectiveness of the security work performed across Facebook, including providing resources to Facebook 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 Facebook's Board of Directors.

Facebook'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 Facebook 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 Facebook groups dedicated to security. The most up-to-date policies and procedures are available to Personnel via Facebook'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. Facebook 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
- Incident Response
- Security, Compliance, Policy and Risk
- Third-Party Security
- Vulnerability Management

Policies within each of these areas create the overall framework that Facebook uses to secure systems across the environment. Responsibility and accountability for management of Facebook'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 a semi-annual basis the Internal Audit (IA) team meets with different teams within Facebook such as the Security Team, Legal, Tax, etc., to understand threats to Facebook 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 six months. The semi-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 Facebook 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. Facebook 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 Facebook 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, ISO27018) and other non-compliance audits to ensure 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 ensure that appropriate controls are in place to mitigate identified risks.

Information and Communication

External Communication

A description of Facebook's systems and services is available to users through the Facebook website. Facebook 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 Facebook Terms and Policies page and help center. There is also a formal process for contacting Facebook with questions and concerns which is communicated to users through Facebook's security page (https://www.facebook.com/security).

Internal Communication

Facebook uses various methods of communication to help employees understand their individual roles and responsibilities and to ensure that events are communicated in a timely manner.

Policies and procedures are in place for employees and these policies are made available to employees through the Facebook 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 Facebook employees via internal Facebook 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 Facebook organization that specialize in designing, developing, implementing, operating, maintaining, and monitoring each respective product to meet Facebook'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 Facebook 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 Facebook organization including the following:

- Engineering: Pulled from the existing Facebook 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 Facebook 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 Facebook platform and associated control environment.

Facebook Enterprise Engineering Team

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

Facebook Global Physical Security Team

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

Facebook Infrastructure Team

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

Community Operations Team

The Community Operations team is responsible for building and preserving trust in Facebook. Key responsibilities include developing scaled solutions for user issues and analyzing how users interact with products and each other.. The team also maintains user safety by identifying and resolving instances of abuse and breach of Workplace's Acceptable Use Policy..

Procedures

Security Domains

Facebook designed the CISP along security domains ("Security Domain(s)"), each of which includes policies and/or safeguards that guide Facebook's security practices. The Security Domains cover key components of how Facebook protects its Information Systems. Facebook takes into account industry standards when developing and benchmarking the policies and safeguards in the Security Domains. The Security Domains help Facebook implement and maintain a program that is designed to support Facebook's commitment to security, availability and confidentiality. The Security Domains in the CISP are:

- Asset Management
- Business Continuity and Disaster Recovery
- Change Management
- Security Compliance, Policy and Risk
- Configuration Management

- Data Security
- Identity and Access Management
- Logging and Monitoring
- Network Security
- People Security
- Physical and Environmental Security
- Security Incident Response
- Third-Party Security
- Vulnerability Management

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

Asset Management

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

Business Continuity

Facebook 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 Facebook's business continuity program.

Each Facebook managed site, office, data center, and region have a Site Resiliency Team 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 Team 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 and continue operations following a disruption. In addition, teams can conduct their own exercises with guidance from the Global Resiliency Team.

The Resiliency program which focuses heavily on the people and process side of things and supplements Facebook's Disaster Recovery efforts, which focus on the resiliency of the Company's network, IT, and engineering assets.

Additionally, to limit exposure from a business continuity event, Facebook 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.

Facebook 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 CapEx over a period of 2-7 years into the future with a goal to also provide forward guidance for the management team to understand upcoming expenses for building out Facebook Infrastructure. The LRP process is visited at least on an annual basis and involve multiple teams and 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 Facebook can handle the planned amount of demand based on the current planned supply.

Disaster Recovery

Facebook has a dedicated team to strategize and improve Disaster Recovery (DR) capabilities to make 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 ensure Facebook and its family of apps stay resilient despite site outages.

Disaster Recovery exercises are conducted to verify Facebook 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

Facebook maintains controls designed to ensure that code changes follow approved procedures and are tracked through version control tools. Facebook uses a formal process and internal tracking system to review, push, and track code changes. Every change goes through the following process:

Change Initiation and Logging

To initiate a change, the change author first creates a differential, or ‘diff’ which documents the proposed changes, test plans for the proposed change, results of the automated testing, and review and approvals. Each diff represents a change to the code base that a developer has proposed for use in production. Developers check out the code base from a central repository and load it into a testing environment in order to test the proposed change.

Human Code Review and Testing

After the code is modified by the author in the development environment, it is submitted for peer review. After completing the review, the peer reviewer, who must be different from the author, can approve the updated code or reject it and request for further modification 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. Testing and approval of the diff are logged by the system to support the code change.

In emergency situations, Personnel may land a change without peer review and testing. However, a retroactive review of such changes is conducted.

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 Facebook Personnel, where the change is tested before being released to the Facebook 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 Facebook'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 Facebook’s internal production instances in order to ensure code developed will work appropriately. Facebook has implemented several measures as described below to ensure data is protected throughout the development process including:

- Training on Facebook'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, including root cause analysis and corrective action for identified issues.
- Dev servers receive the same level of security configurations across the tech stacks as production systems.

Production Code Push

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

Additionally, users with access to push Workplace client code to the mobile application stores are reviewed to validate the appropriateness of active access based on user job duties and employment status.

Secure Coding

Facebook has secure development and coding processes in place for the design and implementation of code changes. In addition, Facebook has developed an expansive set of libraries which automatically implement secure coding standards when they are used by developers. Engineers receive training on Facebook's coding standards during engineering Bootcamp.

Security Compliance, Policy and Risk

Compliance

Facebook 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 Facebook systems. Our security framework is built on our Common Control Framework (CCF). The CCF is a comprehensive set of applicable control requirements that have been rationalized from several different industry information security standards (e.g. ISO/IEC 27001:2013, NIST CSF, SOC2 trust service categories etc.). Facebook reviews this framework periodically to ensure it is aligned with both Facebook's business processes and requirements based on internal company feedback, customer requirements and guidance from industry and regulatory bodies. In addition, Facebook conducts regular assessments of compliance with security policies, frameworks, and regulatory requirements.

Policy

Facebook maintains a suite of information security policies based on a standard policy framework. 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. Facebook 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 and support the appropriate protection against the unwanted disclosure, modification, or destruction of Facebook 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.

The Facebook Security Team has further developed a dynamic risk assessment program in response to the environment in which Facebook operates. The team tracks and manages risks identified from multiple sources including the team's expertise and experience, risk assessment activities, security monitoring tools, key external resources, and company-wide incident management response systems. Outputs from the risk assessment activities are communicated to relevant management and stakeholders, including 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 a number of operational monitoring and evaluation processes 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 Team to support the teams in the identification and mitigation of potential threats to Facebook'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 Facebook 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 Facebook employees.

Security Governance

Facebook 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 wiki site that is available to all employees.

Data Policies and Terms of Service

Facebook communicates its security and confidentiality commitments and obligations to enterprise users and companies via the workplace agreement Terms of Service and Data Policy.

System Design Documentation

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

Configuration Management

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

Data Security

Data and Data Classification

Facebook 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, i.e. within the company.
- Private/Confidential data has a reasonable expectation of privacy and/or confidentiality. It is intended for limited audiences, even within the Company. For some data types and/or use cases, additional restrictions apply.

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

To facilitate deletion, Facebook has a data deletion framework that ensures data and associated user data is deleted appropriately. Deletion scripts run at a defined frequency to ensure data is deleted 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.

Facebook 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 (e.g., 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.

Data Ownership

Workplace from Facebook is segregated into separate and privately managed communities. This segmentation is facilitated by the same technology that enforces Facebook’s core privacy features and controls within Facebook’s public platform. When an enterprise signs up for Workplace, Facebook creates a unique enterprise identifier. All data created by enterprise administrators and users within that enterprise’s managed community are associated to that respective enterprise ID, thereby protecting the confidentiality of that data.

The initial setup is facilitated by Facebook to ensure that the core security and experience features function appropriately, but after the initial setup, the enterprise is solely responsible for managing user access, data deletion, data retention, and content moderation until the enterprise terminates services. The Workplace from Facebook product has available tools to help enterprise administrators manage and control their data.

As a result of this structure, the enterprise owns all data produced and maintained within the managed community while Facebook provides the platform.

CDN Data Encryption

Cached content on globally distributed CDN infrastructure (e.g. Photos, videos, other cached objects) is encrypted at rest on storage media to reduce the risk of data loss when storage media is moved out of controlled environment

Endpoint Security

By default, Facebook uses TLS to encrypt all users' interactions with Facebook and each respective product irrespective of whether these interactions are made via a browser or the API. The digital certificates, used to provide the TLS encrypted connection between Facebook 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.

Facebook laptops are protected via full disk encryption and anti-malware solutions. Facebook relies on endpoint instrumentation to detect and respond to potential compromises of endpoints. Facebook's endpoint security products feed data into log aggregation and alerting systems that the Security Team uses to monitor for evidence of compromise. Laptops are kept in compliance with Facebook's security configuration standards using centralized management tools that are also used to deploy patches and updates. Additionally, Facebook 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 Facebook Personnel

Upon joining Facebook, 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 Facebook's Human Resources system to create associated Active Directory and LDAP UNIX accounts in the system. Access to development servers is authenticated 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).

From development servers (dev servers), authorized users can access production servers via SSH using a certificate issued on the dev server. Authorized users can generate a certificate from the Facebook Certificate Authority (CA) which expires in a pre-defined time based on their job role or pre-approval. Access to a tier is restricted to specific authorized groups, users and services. Only authorized maintainers can add new users to these groups and/or services. In addition, group membership and Access Control List (ACL) configurations to product related access groups are reviewed on a quarterly basis for appropriateness.

Facebook uses a variety of encryption techniques to protect data in transit. Internally, Facebook uses encrypted protocols (including SSH and HTTPS) for system management and access to production. When not connected to Facebook's corporate network, remote access is provided via a TLS encrypted Virtual Private Network (VPN) or from a managed device through managed gateways and requires two-factor authentication. Facebook 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 Human Resources 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 Enterprise Admins and Users

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

Logical Access for Customers

By default, Facebook uses Transport Layer Security (TLS) to encrypt all users' (including customers) interactions with Facebook. The digital certificates, used to provide the TLS encrypted connection between Facebook and the user, are by a trusted Certificate Authority and are current i.e. not expired.

On a need-to-know basis, engineers and teams supporting Workplace products may access Workplace data (e.g., 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. Facebook has a zero-tolerance approach to abuse, and improper behavior results in termination.

Logging and Monitoring

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

Facebook’s internally built intrusion detection system is used to collect and monitor logs from production and corporate systems. Facebook also utilizes endpoint-monitoring software to log and monitor activity on Facebook-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 ensure systems are consistent with expected security standards.

Facebook 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, Facebook 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. Facebook uses a cutting edge Berkeley Packet Filter (BPF) based DDoS mitigation capability.

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

Facebook's mission is to give people power to build community and bring the world closer together. Facebook Human Resources helps drive that mission through finding, growing and retaining the best people who are committed to that mission. Aligned with Facebook's focus on protecting its users from all manner of threats, Human Resources understands that this starts with the people Facebook 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, Facebook employees and contingent workers are required to complete background checks during their onboarding process. Facebook monitors and reviews progress reports to ensure completion of background checks, prior to being granted access to FACEBOOK worksites and Information Systems, including FACEBOOK-issued Devices or physical access tokens (e.g., ID badges, hardware-based multi-factor authentication tokens. If Facebook identifies a candidate has not completed the background checks, then notification and escalation procedures are enforced in accordance with the Facebook Background Check Policy.

Facebook employees and contingent workers are required to sign a confidentiality statement upon hire agreeing to the terms set forth in Facebook'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 on-boarding process.

Finally, Facebook 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) Facebook'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

Facebook maintains policies for the appropriate use of electronic communications by Facebook personnel. These policies set restrictions regarding the content of messages sent by Facebook personnel, disclosure of privileged communications, endorsements, public representations, spam, and intellectual property. These policies also advise employees of Facebook'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 Facebook employees and contingent workers.

Privacy and Security Awareness Training

New and existing Facebook 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 Facebook's key privacy principles, Facebook'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 Legal Learning Operations team performs weekly monitoring to ensure employees receive and take their mandatory training. Legal Learning Operations enforces notification and escalation procedures for participants identified as not having completed training assignments.

Facebook's Security Team conducts an annual, month-long security awareness campaign called "Hack-tober." The month includes hacks, where the Security Team targets Facebook employees and where the employees target the Security Team, security scavenger hunts looking for bugs in code, presentations from internal and external speakers, and an internal security capture the flag.

Additionally, Facebook'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 Facebook is facing. Facebook also encourages Security Team members to attend security conferences hosted outside 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 Facebook standards, and practices, and to develop their technical skills so that they have the right resources to fulfill their responsibilities which includes different training tracks available during the onboarding process. These options provide individuals with general training as well as role specific training necessary to understand the Facebook environment. This includes guidelines on Facebook’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 Facebook Premises and Data Centers

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

- North America
    - Altoona, Iowa
    - Ashburn, Virginia
    - Forest City, North Carolina
    - Fort Worth, Texas
    - Henrico, Virginia (from March 2020)
    - Loudon, Virginia (from July 2020)
    - Los Lunas, New Mexico
    - New Albany, Ohio
    - Prineville, Oregon
    - Santa Clara, California
    - Papillon, Nebraska

- Europe
  - Clonee, Ireland
  - Odense, Denmark
  - Luleå, Sweden

Access to Facebook facilities is restricted through badge access, monitoring through the use of CCTV cameras and by guard staff 24x7. 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 Facebook facilities. Facebook Premises are controlled through badges issued to Facebook personnel (including employees, interns, contingent workers, and vendors). Internal resources are provided to support compliance with badge access policies, and Facebook 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. Facebook 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 Facebook, 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 Facebook premises.

Facebook 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, Facebook has onsite data center managers who conduct monthly facility access reviews and review the data center leasing companies' applicable audit reports. These processes ensure that access to Facebook cages and suites in third party data centers are authorized and appropriate and that the controls implemented are designed and operating effectively and data centers meet Facebook security and availability and confidentiality commitments.

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

In addition to maintaining strong physical security standards at owned locations, Facebook 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 Facebook owned and leased data center locations, temperature and humidity levels are maintained and monitored at appropriate levels. Facebook 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. Facebook owned data center facilities have adequate redundant secondary power (UPS/CPS), backup generator units and tele-communications to support critical systems in the event of a utility outage.

Data Disposal

Facebook has a process in place for 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 Facebook. Electronic media does not leave Facebook's chain of custody without documented proof or 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 Facebook incident management system and assigned a severity level. The Incident On-Call team will evaluate each incident ticket in the Facebook 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

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

Security Incident Reporting and Resolution

Facebook 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 Internal Detection & Response 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 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.

Facebook 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, 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 to identify security threats through periodic vulnerabilities and penetration testing.

Externally Reported Threats and Vulnerabilities

Facebook also has processes in place for external parties to communicate identified issues to Facebook. These primarily include the bug bounty program and via the Help Center Operations Team. Customers are encouraged to report security issues via https://www.facebook.com/whitehat

The bug bounty program encourages external users to report any security vulnerability that they find. The Company has a designated on-call team who manages the review and validation of white hat reports. Once a case has been validated, resolution of the issue is determined based on the severity level and a ticket is created in Facebook’s internal system to track and document the resolution.

Third Party Security

Third Party Security Program

Any third party that performs front-office or back-office operations, manufactures hardware devices for Facebook, or requires access to sensitive company data or integration with corporate systems must submit to a security assessment and agree to appropriate contractual provisions prior to their being retained. Third party security assessments are conducted by Facebook 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 nature of anticipated connectivity with Facebook.

Third Party Security Assessments

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

Facebook'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 Facebook's commitments to protect user data. As part of the due diligence process, Facebook asks prospective third parties to complete a third party security questionnaire to assess whether the third party meets Facebook's functional security requirements to protect the privacy and confidentiality of user data. The questionnaire is targeted to obtain 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; and
- What types of data the third party collects and how this data is being collected

Based upon the third party's responses to the third party security questionnaire and other data points, Facebook's Security Team determines whether further security assessments are required. Facebook often partners with an outside security consulting firm to conduct security assessments, which may include testing of the third party's controls, a vulnerability scanning program, a web application penetration test, and/or a code review for security defects. When employed, the security-consulting firm reports its findings to Facebook, and Facebook requires that the prospective third party fix critical issues before being on-boarded. Depending on the sensitivity of Facebook data shared with the third party and other factors, Facebook may require that the third party undergo a periodic or random security and/or privacy assessment. Third Parties are classified as Low, Medium, High, or Critical Risk, which, in turn, determines the approval status as Recommend (Low and Medium), Recommend Conditionally (High), or Do Not Recommend (Critical Risk). In the event a Third Party is given a "Recommend Conditionally" approval status, the Third Party must agree to the conditions provided by the Facebook Security Team. If the Facebook Security Team gives a Do Not Recommend approval status to a Third Party, the decision whether to continue onboarding the Third Party is escalated to the Business and Legal teams.

Facebook also has a contract policy (the “Contract Policy”), which governs the review, approval, and execution of contracts for Facebook. Facebook’s pre-approved contract templates require third parties to implement and maintain appropriate protections for user data. Facebook 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. Facebook Legal documents review of any such contracts through formal approval prior to contract execution.

Software-as-a-Service

Facebook policies govern the use of Software-as-a-Service (“SaaS”) solutions to receive, transmit, store, and process Facebook data. New SaaS solutions that have not previously been subject to a vendor security assessment must complete an assessment.

Vulnerability Management

Facebook 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 at least on a quarterly basis 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. On a periodic basis the Vulnerability Management Team posts an update detailing the scans runs, trends or types of vulnerabilities identified, remediation action taken, current open tasks, roadblocks, etc. 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, Facebook 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. Our data centers continue to operate; however, in light of the reduced levels of staffing, we have increased the response time for physical security staff to respond to alarms and have postponed scheduled maintenance of data center equipment. In an instance where we have postponed maintenance, we have obtained a documented exception.

Complementary User Entity Control Considerations

The Workplace from Facebook 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 Facebook 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
• CUEC 1 – User entities are responsible for maintaining appropriate documentation supporting the appropriate use of Workplace from Facebook, as needed by their users, administrators, and auditors.	CC2.3
• CUEC 2 - User entities are responsible for managing access configurations within Workplace from Facebook to appropriately assign access to their users.	CC6.1 CC6.2 CC6.3
• CUEC 3 - User entities should establish, monitor and maintain sufficient internal controls to ensure appropriateness of access to their Workplace Instances.	CC6.2 CC6.3
• 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.	CC6.2 CC6.3
• CUEC 5 - User entities should review security access and authorization limits on a periodic basis and monitor all user access and authorization limits.	CC6.2 CC6.3
• CUEC 6 - User entities are responsible for timely notification to Facebook of changes to authorized administrators on their enterprise account.	CC6.1 CC6.2 CC6.3
• 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 Facebook.	CC6.1

• CUEC 8 - User entities are responsible for the secure handling and storage of any administrative access tokens generated for use with relevant Workplace from Facebook APIs.	CC6.1
• CUEC 9 - User entities are responsible for ensuring physical access controls are in place to protect their machines accessing Workplace from Facebook.	CC6.4
• 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.	CC2.3
• CUEC 11 - User entities are responsible for communicating any bugs or processing issues discovered to Facebook.	CC7.1 CC7.2
• CUEC 12 – User entities are responsible for requesting data deletion in line with their requirements.	C1.1 C1.2
• CUEC 13 - Facebook does not provide an archiving service, and user entities are solely responsible for creating backups of Their Data.	C1.1 C1.2

The list of complementary user entity control 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

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

Security, availability and confidentiality commitments to user entities are documented and communicated in the Facebook 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 Facebook systems. Support request initial response times are based on Workplace plan.

Facebook 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 Facebook'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.

Facebook 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 Facebook 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 Facebook website and in the complementary user entity controls (CUEC) section of the report.

Attachment C – Workplace from Facebook Product and the General Data Protection Regulation (GDPR)

Workplace from Facebook and the General Data Protection Regulation (GDPR)

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.

For Workplace, our customers are the data controller in respect of the personal data on their Workplace instance. They appoint Facebook as their data processor under the Workplace agreement and instruct Facebook to process their users' personal data pursuant to the Workplace agreement.

For more information see http://www.workplace.com/workplace/blog/workplace-and-gdpr

Safeguards and Contractual Commitments

GDPR requires data controllers to engage data processors with appropriate safeguards, in order to 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.

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.

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

Workplace and Oculus for Business

Oculus for Business extends workplace platform and offers a secure and reliable VR solution for enterprise customers. The offering includes software to set up and manage VR deployments, a tailored in-headset experience and enterprise-grade customer support.

Device Manager an asset management solution built on top of Workplace allows customers of Oculus for Business see the status on each head-set and lets you change settings, group devices and bulk-apply settings and more.