Cloud Software Group Services Security Exhibit

Effective April, 2026

Contents

Purpose **3**
1. Scope **3**
2. Security Program and Policy Framework **3**
2.1 Security Risk Oversight 3
2.2 Security Risk Management 3
2.3 Information Security 4
Cybersecurity Function 4
Governance, Risk, and Compliance (GRC) function 4
3. Access Management **4**
3.1 New Accounts, Roles, and Access Requests 5
3.2 Account Review 5
3.3 Credentials 5
3.4 Access Management for Customers 6
4. System Development and Maintenance **6**
4.1 Secure Development LifeCycle 6
Security Training & Culture 6
Security Planning and Architecture 6
Advanced Threat Modeling 7
Multi-Tiered Code Analysis 7
Software Supply Chain & Open Source Security 7
4.2 Change Management 7
4.3 Penetration Testing 7
5. Asset Management **7**
5.1 Physical and Virtual Asset Management 7
5.2 Application and System Management 7
5.3 Data Retention 8
6. Human Resources Security **8**
6.1 Background Screening 8

6.2 Training 8
6.3 Phishing/Social Engineering Simulations 8
6.4 Enforcement 9
7. Operations Security 9
7.1 Network and System Security 9
7.2 Logging 9
7.3 Certificate, Credential, and Secret Management 9
7.4 Vulnerability Management 9
8. Encryption 10
9. Physical Security 10
9.1 Facilities 10
9.2 Data Centers 11
10. Business Continuity & Disaster Recovery 11
10.1 Business Continuity Plan (BCP) Overview 11
10.2 Disaster Recovery (DR) Overview 12
10.3 Crisis management Plan (CMP) Overview 12
11. Incident Response 12
12. Vendor Management 12
12.1 Onboarding 12
12.2 Ongoing Assessment 12
12.3 Off-boarding 12
13. Compliance 13
13.1 Treatment of Personal Data 13
13.2 Disclosure of Customer Content 13
13.3 Customer Security and Regulatory Requirements 13
14. Customer Audits and Inquiries 13
15. Contacts 14

Purpose

This Cloud Software Group Holdings, Inc. (“Cloud Software Group”, “we”, “us” or “our”) services Security Exhibit (the “Exhibit”) describes the security controls implemented in connection with the performance of software, cloud services, technical support services, or consulting services (the “services”) delivered to customers (“Customer”, “You” or “Your”) under the relevant order for the products or services (collectively, the “Agreement”). Beta or lab/tech preview products or services (including Cloud Labs) and Our internal IT systems not involved in the delivery of services are outside of the scope of this Exhibit.

1. Scope

This Exhibit describes the administrative, physical, and technical security controls we employ in order to maintain the confidentiality, integrity, and availability of our services. These controls apply to our operational and services systems and environments. Cloud Software Group employs ISO/IEC 27001 as the baseline for its services security program and has obtained industry certifications and assessments for specific services. Additional information relating to current Certifications is available on our Trust Center https://www.cloud.com/trustcenter/certifications.

We seek to continually strengthen and improve our security practices, and reserve the right to modify the controls described herein. Any modifications will not diminish the level of security during the relevant term of services.

2. Security Program and Policy Framework

Cloud Software Group has a security program and policy framework that is established and approved by senior and executive management representing various business areas throughout the company. Policies are reviewed annually and updated as needed to current industry good practice.

2.1 Security Risk Oversight

The Cyber Risk Oversight Committee (CROC) governs security risk management activities. The CROC consists of cross-functional management and leadership. The executive leadership team reviews committee membership on an annual basis to confirm adequate coverage of business and operational areas.

The CROC meets at least quarterly and provides guidance, insight, and direction in identifying, assessing, and addressing security risks in both corporate operations, as well as service delivery infrastructure.

2.2 Security Risk Management

Cloud Software Group utilizes a Security Risk Management (SRM) program that identifies potential threats to our services and to our infrastructure, rates the significance of the risks associated with those threats, develops risk mitigation strategies, and partners with our Product and Engineering teams to implement those strategies. Our risk management program aligns with ISO 31000, NIST SP 800-171 and ISO/IEC 27005, and outlines Cloud Software Group's Cybersecurity Risk Management program, which aims to strengthen our security posture by identifying, assessing, prioritizing, and treating security compliance-related risks. The program is overseen by the Cloud Software Group GRC team and governed by the CROC.

Key aspects of the program include:

- **Purpose:** To protect Cloud Software Group from losses (financial, intellectual property, operational, reputational) by managing security and compliance risks.
- **Scope:** Applies to all departments and business units within Cloud Software Group's Information Security Policy.
- **Risk Assessment Methodology:** Uses an iterative approach (Identify, Analyze, Evaluate) to manage security risks, with assessments occurring at least annually.
    - **Identify:** Focuses on identifying assets, vendors, threats, vulnerabilities, and existing controls.
    - **Analyze:** Calculates risk based on the estimated impact (Low, Medium, High) and likelihood (Unlikely, Possible, Likely) of a threat.

    - **Evaluate:** Assesses the effectiveness of existing security controls.
- **Risk Treatment and Acceptance:** Involves assessing current controls, applying treatment options (Accept, Mitigate, Share, Transfer, Avoidance), and obtaining approval from the CROC for risk acceptance. Remediation plans have SLAs that are in line with our Risk Management Policy.
- **Risk Monitoring:** Continuous monitoring of risk factors, control effectiveness, and treatment plans, with risks tracked in a Risk Register. General updates are provided to the CROC quarterly.

2.3 Information Security

Cloud Software Group has appointed a Chief Information Security Officer (CISO), who is responsible for security oversight and policy strategy, compliance, and enforcement.

The CISO also leads the Governance, Risk & Compliance (GRC), and the Cyber Security teams. These teams are responsible for the Cybersecurity and (GRC functions detailed below.

Cybersecurity Function

The **Cybersecurity** function is responsible for implementing technical and operational security controls to protect the organization's IT infrastructure, applications, data, and systems from threats and vulnerabilities.

- **Vulnerability Management:**
  Conduct ongoing identification, classification, remediation, and mitigation of vulnerabilities in systems, applications, and infrastructure. This includes patch management and regular security scanning.
- **Vulnerability Assessment and Penetration Testing (VAPT):**
  Manage and execute internal and external VAPT activities, ensuring secure configurations and identifying exploitable weaknesses in the environment.
- **Security Operations Center (SOC) Monitoring:**
  Oversee real-time monitoring of security events and alerts. Coordinate with the SOC team to investigate incidents, perform root cause analysis, and escalate as needed.
- **Third-Party Risk Management (TPRM):**
  Evaluate the security posture of third-party vendors and service providers. Implement risk-based onboarding, periodic assessments, and continuous monitoring of vendor security practices.

Governance, Risk, and Compliance (GRC) function

The GRC function ensures we adhere to regulatory and contractual requirements while promoting transparency, managing risk, and driving a culture of security awareness. It is composed of three specialized teams:

- **Customer Security Assurance:**
  Responsible for managing customer security assessments, responding to security questionnaires, maintaining the Trust Center, developing customer-shareable security documentation, and supporting customer-performed audits.
- **Compliance Management:**
  Oversees internal and external audits, maintains compliance with regulatory and certification standards, and manages the organization's risk and issues register.
- **Security Compliance Training:**
  Develops and delivers general security awareness and role-based training programs, ensuring employees understand and fulfill their security responsibilities.

Cloud Software Group has Information Security policies and standards to define security requirements. These security policies and controls are detailed in the clauses below.

3. Access Management

We require the use of access control measures designed to ensure appropriate privileges are assigned and maintained for access to company systems, assets, data and facilities in order to protect against potential damage, compromise, or loss. We follow the Least Privilege Principle, and/or role-based security, limiting user's access to only what is necessary to perform job functions or roles.

Managers design roles to provide adequate separation of duties, distributing tasks and privileges among multiple people in order to safeguard against fraud and error.

3.1 New Accounts, Roles, and Access Requests

Cloud Software Group requires a formal request for access to company systems or data. Each access request requires a minimum approval of the user's manager to confirm the user's role and access. Access administrators confirm that necessary approvals are obtained prior to granting access to systems or data. The principle of least-privilege is applied.

3.2 Account Review

We perform, at minimum, annual reviews of user and privileged accounts and assigned permissions for key systems and functions. Any changes are actioned promptly.

3.3 Credentials

Cloud Software Group's passwordless authentication system introduces a stronger and more secure verification method by removing the need for users to enter traditional passwords during login. Users authenticate through a mobile device using an authentication app. At login, the application displays a unique QR code, which the user scans with the app. The app then performs a cryptographic identity verification, and upon successful validation, a time-limited access token is issued to complete the login.

Although this provides a password-free experience for the end user, a password is still maintained on the backend for account administration and lifecycle purposes. By eliminating the need for user-entered passwords during authentication, we significantly reduce common risks such as password theft, phishing, credential reuse, and brute-force attacks. This approach provides a higher level of assurance and aligns with, or exceeds, modern security expectations outlined in standards such as PCI DSS, ISO 27001, and NIST.

3.3.1 Password Management

In addition to passwordless authentication, Cloud Software Group also maintains a formal Password Policy to govern the secure handling and administration of all account passwords, where applicable. These practices include:

Minimum Password Age: A minimum age of 1 day is enforced to prevent users from rapidly cycling through passwords or reverting to previously used credentials.

Password Change Interval: Passwords for standard/test accounts and administrative/privileged accounts must be changed every 90 days to reduce the risk of long-term compromise.

Password History: A history of the last 24 passwords is maintained to prevent reuse and ensure each new password is unique and resistant to guessing or cracking.

Invalid Logon Attempts & Account Lockout: A maximum of 6 failed logon attempts is allowed within a 30-minute window. Exceeding this limit triggers an account lockout until reset by an administrator, mitigating brute-force attempts.

Password Complexity Requirements: All passwords must meet defined complexity standards, including:

- Exclusion of common or dictionary words
- Prohibition of using user IDs or email addresses

- Disallowing three or more sequential or repeating characters

Differentiated Security Measures - Minimum Length:

To reflect the varying risk profiles of user accounts, minimum lengths are enforced as follows:

- **Standard/Test Accounts:** Minimum of 12 characters
- **Administrative/Privileged Accounts:** Minimum of 14 characters for increased entropy and protection of sensitive systems
- **Non-user / System / Service accounts:** Minimum of 16 characters

These requirements strengthen resistance against cracking and unauthorized access, especially for high-privilege accounts.

Secure Handling of Passwords: Cloud Software Group maintains the confidentiality and integrity of passwords through measures such as:

- Ensuring passwords remain hashed or encrypted throughout their lifecycle
- Prohibiting password sharing

Together, these authentication and password management controls provide a strong, layered approach that protects user accounts, supports secure operations, and aligns with industry best practices.

3.4 Access Management for Customers

Access Management of customer accounts are fully managed by the customers.

On-premises products: Since these are deployed within customer-managed environments, customers host the application infrastructure themselves and therefore retain complete control over all aspects of access management, including authentication, authorization, password policies, and integration with internal identity systems.

Cloud products: Customers have full control over user and access management to their cloud-hosted products through standard identity protocols such as SSO, SAML, and LDAP. Customers can enforce their own password management policies, including complexity, rotation, and reset requirements. Cloud Software Group does not impose centralized authentication, allowing customers to manage access and password controls according to their internal security and compliance standards.

4. System Development and Maintenance

Cloud Software Group employs a comprehensive Secure Development Lifecycle (SDL) governed by specialized security practitioners. This program enforces strict change control procedures, validated security requirements for all information systems, and the sanitization of data within test environments. The security team provides continuous oversight through formal design validation, structured threat modeling, and a combination of automated and manual security testing, including annual penetration testing.

4.1 Secure Development LifeCycle

Cloud Software Group employs a formal Secure Development Lifecycle (SDL) to govern the acquisition, development, and maintenance of all information systems. Our security policy is built on an integrated SDL, where the Product Security team acts as a strategic partner to Engineering, ensuring security is a foundational requirement.

Security Training & Culture

We maintain a continuous, competency-based security training framework for our Engineering community. This curriculum covers advanced topics including threat modeling methodologies, secure design, secure coding patterns. All Engineers must re-verify their security proficiency annually to maintain organizational awareness.

Security Planning and Architecture

Aligned with the Scaled Agile Framework (SAFe), Product Security engages during the initial planning phase of every development cycle. By performing early-stage Security Impact Assessments on new features and architectural changes, we ensure that security requirements are included by design.

Advanced Threat Modeling

We proactively identify and mitigate design-level risks through structured threat modeling. These collaborative sessions analyze system interactions to define the attack surface, identify high-value assets, and implement counter-measures before coding.

Multi-Tiered Code Analysis

Feature implementations are subject to a security review process:

- **Manual Security Reviews:** Mandatory for high-risk components, including authentication/authorization flows, multi-tenancy isolation, memory management, and cryptographic implementations.
- **Automated Static Analysis (SAST):** Industry-standard tools are integrated directly into our CI/CD pipelines, providing real-time feedback to developers and catching common vulnerabilities early in the commit cycle.

Software Supply Chain & Open Source Security

To ensure the integrity of our software supply chain, we utilize Software Composition Analysis (SCA) tools integrated into our build pipelines.

- **Vulnerability Monitoring:** We maintain continuous visibility into third-party and open-source dependencies, enforcing strict policies regarding vulnerability thresholds and license compliance.
- **Open Source Governance:** A dedicated software-based system manages the approval and auditing of all open-source components, supported by documented policies and developer-specific best-practice training.

4.2 Change Management

Our infrastructure and software change management process addresses security requirements and requires that software and infrastructure changes to be authorized, formally documented, tested (as applicable), reviewed, and approved prior to deployment to the production environment. Infrastructure and software changes are managed and tracked using work management systems. The change management process is appropriately separated, and access to migrate changes to production is restricted to authorized personnel.

4.3 Penetration Testing

Penetration testing of Cloud Software Group systems is conducted via an independent team. Both enterprise testing and select product testing is performed annually. Issue ratings shall follow industry standard practices. We also use the Common Vulnerability Scoring System (CVSS) published by the US National Institute of Standards and Technology (NIST) for rating vulnerabilities. Findings from the penetration test will be addressed according to established company security policy.

5. Asset Management

5.1 Physical and Virtual Asset Management

Cloud Software Group maintains a dynamic inventory of the physical and virtual systems we manage and use to perform the services (“Service Assets”). System owners are responsible for maintaining and updating their Service Assets consistent with our security standards. Formal disposal procedures are in place to guide the secure disposal of Cloud Software Group and Customer Content. We dispose of data when no longer required based on classification and using deletion processes designed to prevent data from being reconstructed. Our technology assets are sanitized and disposed of when they are no longer needed within their designated or assigned area. Technology assets include but are not limited to individual computing devices, multifunction computing devices, storage devices, imaging devices, and network appliances.

5.2 Application and System Management

Application and system owners are responsible for reviewing and classifying the data they store, access, dispose of, or

transmit. Among other controls, employees and contractors are required to:

- Classify Customer Content as among the highest two categories of Cloud Software Group confidential information, and apply appropriate access restrictions;
- Restrict the printing of Customer Content and dispose of printed materials in secure containers;
- Not store corporate or Confidential Information on any equipment or device that does not meet the requirements of Cloud Software Group security policies and standards; and
- Secure computers and data while unattended.

5.3 Data Retention

Customer Content stored as part of our Cloud services is accessible by the Customer for 30 days following the termination of services. Additional details are provided in the specific services documentation. Customer Content may also be retained following the completion of the services if required for legal purposes. Cloud Software Group will comply with the requirements of this Exhibit until such Customer Content has been permanently deleted.

We will provide written confirmation of deletion upon request.

6. Human Resources Security

Maintaining the security of Customer Content is one of the core requirements for all employees and contractors. Our Code of Business Conduct requires all employees to adhere to our security policies and standards, and specifically addresses the protection of confidential information, as well as personal information of customers, partners, suppliers, and employees. All employees and contractors are subject to confidentiality agreements, acceptable use, and privacy requirements that cover customer information. The Cloud Software Group Security organization also regularly communicates to employees and contractors on topics related to information and physical security in order to maintain security awareness on specific topics.

6.1 Background Screening

We currently use background screening vendors for all new hires globally and require the same for our third-party supplier personnel, except where limited by local law or employment regulations.

6.2 Training

All employees and contractors are required to complete data protection and role-based security training upon hire, and annually thereafter, or as required by compliance obligations. This training covers company policies designed to protect confidential information, including that of our customers, partners, suppliers, and employees.

The program includes guidance on security and privacy practices and principles for handling confidential data, emphasizing appropriate use, access, sharing, and retention. Engineering team members receive additional training focused on secure development, architecture, and coding practices.

These training programs require participants to acknowledge security and privacy policies and to pass quizzes with a minimum score to receive a completion certificate.

6.3 Phishing/Social Engineering Simulations

We conduct phishing simulation campaigns on a periodic basis as part of our ongoing security awareness program. These simulations are designed to assess employee vigilance, reinforce secure behaviors, and identify areas where additional awareness may be needed.

Employees who interact with a simulated phishing email (e.g., clicking a link or submitting information) are enrolled in targeted remedial training. This training focuses on recognizing phishing attempts, safe email practices, and reporting procedures. Completion of the training is tracked to ensure accountability.

The program is continuously monitored, and results are reviewed to identify trends, strengthen controls, and improve overall organizational resilience against social engineering threats.

6.4 Enforcement

All employees and contractors are required to comply with our security and privacy policies and standards. Non-compliance is subject to disciplinary action, up to and including termination of employment.

7. Operations Security

7.1 Network and System Security

Cloud Software Group has documented network and system hardening standards designed to ensure that networks and systems are securely configured. Required procedures under these standards include, but are not limited to:

- Changing or disabling default settings and/or accounts;
- Controlled use of administrative access;
- Restrict service accounts for only the purpose which they were created; and
- Configure logging and alert settings appropriate for auditing.

We require the implementation of anti-malware software on servers and workstations, and scan the network for malicious software.

Network controls govern access to Customer Content. These include, as applicable: configuring an intermediate untrusted zone between the Internet and the internal network that includes a security mechanism to restrict access and unauthorized traffic; network segmentation to prevent unauthorized access of Customer Content; and separating web and application servers from the corresponding database servers in a tiered structure that restricts traffic between the tiers.

7.2 Logging

We collect logs to confirm the correct functioning of our services, to assist with troubleshooting system issues, and to protect and secure our networks and Customer Content. Logs may include access ID, time, authorization granted or denied, diagnostic data such as trace and crash files, and other relevant information and activity.

We collect and use logs (i) for providing, securing, managing, measuring and improving the services, (ii) as requested by customer or its end-users, (iii) for billing, account management, internal reporting, and product strategy, and/or (iv) for compliance with agreements, policies, applicable law, regulation or government request. This may include monitoring the performance, stability, usage and security of the services and related components. Customers may not block or interfere with this monitoring.

For more information on Customer Content and Log handling, please see Our Trust Center which contains several white papers on Cloud Software Group Cloud services Logging.

7.3 Certificate, Credential, and Secret Management

Cloud Software Group maintains policies that cover the lifecycle of certificates, credentials, and secrets to ensure protection, availability, and confidentiality. Secret custodians must be documented and formally acknowledge that they accept the responsibilities as secret management personnel. Responsibilities include, but are not limited to:

- Certificates must be issued by an approved certificate authority;
- Cryptographic keys may not be stored or transmitted in plain text and must use strong approved cryptographic protocols; and
- Credentials, keys and secrets must be rotated at least once per year and stored in an approved privileged authentication management tool.

7.4 Vulnerability Management

We monitor applications and systems for vulnerabilities with automated vulnerability and port scanning on a regular basis. Vulnerabilities identified are required to be remediated on a timeline that is based on the severity rating and the associated risk along with vendor recommendations. In cases that a patch, update, or permanent mitigation is not available, appropriate countermeasures will be used to reduce the risk of exploitation of the vulnerability without undue delay

Cloud Software Group also has a public bug bounty program on HackerOne that provides a pathway for researchers to submit

findings in a number of our Products. We believe the researcher community to be an extension of the security functions performed within the organization and look to engage with the community through regular outreach.

Product Security Incident Response

Cloud Software Group takes a comprehensive approach to investigating, addressing, and informing customers of known product vulnerabilities. Cloud Software Group also offers multiple avenues to report product vulnerabilities including a continuously monitored, dedicated inbox, and through our active bug bounty program.

A customer or security researcher may report a vulnerability through our Trust Center's Report a Security vulnerability. The Vulnerability Response section of the Trust Center includes additional details on the program. Cloud Software Group publishes security advisories to provide remediation information about security vulnerabilities in customer-managed Cloud Software Group products which have been reported to us through the vulnerability response program.

Cloud Software Group looks to the issues reported or identified through these avenues as feedback to further improve upon the features and components within Cloud Software Group products and services.

8. Encryption

Cloud Software Group is committed to protecting Customer Content through strong encryption standards, both in transit and at rest. Encryption is a core component of our security architecture, ensuring that confidential information remains protected against unauthorized access across all environments.

8.1 Protection of Data in Transit

All data transmitted over public networks is secured using industry-standard encryption protocols. Customer Content in transit is protected using TLS 1.2 or higher to ensure secure communication between systems and services.

8.2 Protection of Data at Rest

Data at rest is secured using AES 256-bit encryption. All workstations used to deliver services are required to have full disk encryption enabled. Customer Content is never stored on portable devices unless properly encrypted.

Some Cloud Software Group services encrypt specific data elements by default and may offer additional encryption capabilities configurable by the customer. Please refer to the relevant product documentation for more details on supported encryption features.

9. Physical Security

Cloud Software Group prioritizes the physical protection of its facilities and assets to safeguard confidential information and maintain operational integrity. Our physical security controls are designed to restrict access, monitor activity, and ensure a safe environment for employees, visitors, and Customer Content.

9.1 Facilities

Cloud Software Group maintains a robust physical security program to protect its facilities, assets, and personnel through tightly controlled access, surveillance, and monitoring.

9.1.1 Access Control and Entry Management

Access to all Cloud Software Group facilities is strictly limited to authorized personnel using a combination of electronic access

control systems, intrusion detection systems (IDS), security personnel, and continuous CCTV surveillance. Facilities typically feature a single primary entry point, with multiple emergency exits, to balance security and safety requirements.

All employees, contractors, and visitors must wear visible identification badges at all times. Physical access events are logged and monitored continuously for auditing and security purposes. Reception and security staff are responsible for verifying badges, registering and escorting visitors, and enforcing strict visitor supervision policies that regulate conduct, movement, and duration, all requiring management approval.

9.1.2 Facility Layout and Zone Security

Cloud Software Group sites adhere to rigorous security design principles, with areas classified into distinct zones—Public, Cloud Working, Cloud Specialized, and Cloud Secure each enforcing tailored access restrictions and encryption requirements to protect sensitive data. Non-secure spaces such as kitchens, dining areas, and restrooms are intentionally located outside of secure working zones to minimize unnecessary access to sensitive areas.

9.1.3 Surveillance and Intrusion Detection

Intrusion Detection and Prevention systems are deployed to promptly identify and respond to unauthorized access attempts. CCTV cameras monitor building perimeters, entry points, lobbies, loading docks, and secured interior spaces controlled by card readers, while avoiding sensitive or communal areas to respect privacy. CCTV footage is securely stored and managed according to policy.

9.1.4 Access Control System and Reviews

Physical access is managed through Access Control Levels (ACLs) defined by facility and security managers. These ACLs are reviewed quarterly and require dual approvals to maintain strict control and prevent unauthorized access.

9.1.5 Security Operations Center (SOC)

Our Security Operations Center oversees daily physical security operations, including guard coordination, access control, CCTV monitoring, badge issuance, and emergency response management. The SOC maintains up-to-date emergency and routine contact information, ensuring readiness for any Security Incident.

9.2 Data Centers

In addition to the controls described above, for Cloud Software Group owned and managed facilities, we implement additional controls at the data centers.

- We use systems designed to protect against loss of data due to power supply failure or line interference, including global and redundant service infrastructure that is set up with disaster recovery sites.
- Data centers and Internet service providers (ISPs) are evaluated to optimize performance regarding bandwidth, latency, and disaster recovery isolation.
- Data centers are situated in facilities that are ISP carrier neutral and provide physical security, redundant power, infrastructure redundancy, and uptime agreements from key suppliers.
- When we use third-party data centers or cloud services for the delivery of the services, we contract providers that meet or exceed the physical and environmental security requirements of our facilities.

10. Business Continuity & Disaster Recovery

10.1 Business Continuity Plan (BCP) Overview

Cloud Software Group maintains a structured Business Continuity Program (BCP) aligned with ISO 22301 and ISO 27001 standards to ensure essential business functions remain available or quickly recoverable during disruptions such as natural

disasters, cyberattacks, or infrastructure failures. The BCP includes an annual Business Impact Analysis to identify critical functions and risks, informing department-specific continuity plans that define resource needs, recovery objectives, and remote work contingencies. Emergency and facility contingency plans support continuity across all major sites, enabling employees to work remotely if facilities become inaccessible.

10.2 Disaster Recovery (DR) Overview

The Disaster Recovery Plan (DRP) complements the BCP by focusing on restoring IT systems, data, and infrastructure supporting critical business functions. It relies on redundant infrastructure across geographically diverse locations to reduce single points of failure. The DRP outlines clear recovery procedures, team roles, escalation paths, and secure restoration protocols with defined Recovery Time and Point Objectives. Key personnel participate in periodic training and simulations to maintain readiness. The DRP is reviewed annually and updated as needed to reflect changes in technology, business processes, and regulatory requirements.

10.3 Crisis management Plan (CMP) Overview

Cloud Software Group's Crisis Management Plan provides a coordinated response framework to minimize impact and protect employees, operations, and stakeholders during critical incidents. It defines crisis lifecycle phases from detection to recovery and activates a cross-functional Crisis Management Team with designated roles. Predefined communication and escalation protocols ensure rapid information flow to all relevant parties. The plan includes structured coordination through scheduled meetings, situation reports, and decision logs, supported by detailed process guides that are regularly reviewed and updated to maintain effectiveness during crises.

11. Incident Response

Cloud Software Group maintains a comprehensive Cyber Security Incident Response Plan that establishes a structured framework for detecting, reporting, identifying, analyzing, and responding to Security Incidents impacting managed networks, systems, or Customer Content. To ensure operational readiness and the effectiveness of these procedures, we conduct formal Security Incident response training and simulation testing at least annually. This is in accordance with NIST 800-61 Revision 2.

"Security Incident" means unauthorized access to Customer Content resulting in the loss of confidentiality, integrity or availability. If we determine that Customer Content within our control has been subject to a Security Incident, the customer will be notified within the time period required by law. Our notice will describe, where known, the nature of the incident, the time period, and the potential impact on you. We maintain a record of each Security Incident.

12. Vendor Management

12.1 Onboarding

Our Third-Party Risk Management Program provides a systematic approach to managing security risks posed by the use of third-party suppliers. We work to identify, analyze and mitigate security risks prior to engaging in the procurement of such third parties.

Cloud Software Group executes agreements with suppliers to document relevant security measures and obligations consistent with those specified in this exhibit. These obligations are outlined in our Supplier Security Standards.

12.2 Ongoing Assessment

We perform periodic, risk-based security assessments designed to ensure security measures remain in place throughout the supplier relationship. Annual reviews are conducted for critical external suppliers who support the information security requirements of cloud-hosted (SaaS) products and customer-facing services.

Changes to services provided or changes to existing contracts require a security risk assessment to confirm that the changes do not present additional or undue risk.

12.3 Off-boarding

We endeavor to notify the supplier's procurement organization at least 90 days prior to the plan to end a supplier relationship or prior to a contract expiration with a supplier (unless earlier termination is required). The supplier's procurement organization coordinates the termination of the existing relationships to confirm that our corporate data and assets are secured and properly handled.

13. Compliance

13.1 Treatment of Personal Data

Personal data is information that relates to an identified or identifiable individual. You determine the personal data that is included in the Customer Content. In performing the Services, we act as a data processor and you remain the data controller for any personal data contained in Customer Content. We will act on your instructions regarding the processing of such personal data, as specified in the Agreement.

Further information concerning the treatment of personal data subject to the General Data Protection Regulation, including the mechanisms employed for international transfer of such data, is provided in the Cloud Software Group Data Processing Addendum located in the Trust Center.

13.2 Disclosure of Customer Content

We may disclose Customer Content to the extent required by law, including in response to a subpoena, judicial or administrative order, or other binding instrument (each a "Demand"). Except where prohibited by law, we will promptly notify you of any Demand and provide you with assistance reasonably necessary for you to respond to the Demand in a timely manner. Further Details can be found within our Law Enforcement Guidelines.

13.3 Customer Security and Regulatory Requirements

The Services are designed to be delivered within a larger customer IT environment, and so customers retain full responsibility for all aspects of security not expressly managed by Cloud Software Group, including, but not limited to, technical integration with the Services, user access management and controls, and all applications and networks that customers may use in conjunction with the Services.

You remain responsible for determining whether your use of the Services, including providing us with access to any Customer Content as part of the Services, is subject to regulatory or security requirements beyond those specified in the Agreement, including this exhibit. Customers must therefore ensure that they do not submit or store any Customer Content that is governed by laws that impose specific controls that are not included in this exhibit, which may include US International Traffic in Arms Regulations (ITAR) or similar regulations of any country that restricts import or export of defense articles or defense services, protected health information ("PHI"), payment card information ("PCI"), or controlled-distribution data under government regulations, unless specified in the Agreement and applicable Service Description and the parties have entered into any additional agreements (such as a HIPAA Business Associate Agreement) in advance as may be required for us to process such data.

14. Customer Audits and Inquiries

In response to audit requests, Customers must rely upon our Due Diligence Package (DDP) for an updated security package and information. Cloud Software Group provides a comprehensive and regularly maintained DDP as the authoritative source for security and compliance information. This package is designed to meet customer due diligence needs without requiring direct audit access. The Cloud services DDP includes detailed documentation covering our Cloud security program, governance practices, data protection controls, and a completed Shared Assessments' Standardized Information Gathering (SIG) questionnaire, insurance certificate, and Business Continuity Program Overview & Assessment Summary. These documents detail our adherence to key industry and regulatory standards and demonstrate our ongoing commitment to operating within globally recognized security frameworks.

Customers seeking information related to our non-cloud offerings may request access to the Corporate Due Diligence Package, which provides similar transparency into the security posture and compliance practices applicable to our Corporate level practices. Both packages are curated to provide meaningful and actionable information while protecting the confidentiality and

integrity of our internal processes. Access to these materials is available through our Trust Center, contingent upon an active Non-Disclosure Agreement or other documented confidentiality obligations. By centralizing and standardizing security documentation in this way, Cloud Software Group ensures timely, consistent, and scalable responses to customer inquiries.

Additionally, customers may reach out to their Account Managers for assistance in completing security assessment questionnaires or for any follow-up questions or requirements that arise from reviewing the DDP.

15. Contacts

Function Contact Customer Support: https://www.cloud.com/trust-center/support

Reporting a Security Incident & Suspected Vulnerabilities in our service: secure@cloud.com .