SOC 3 +C5

Program: Cisco Webex Meetings.

Webex Messenger, Webex Meetings, Webex Training, Webex Events, Webex Support

For the period

October 13, 2017 to October 12, 2018

Accedere Inc. in association with DNV-GL

DNV·GL

Accedere Inc.

Certified Public Accountants

info@accedere.us

Table of Contents

Section I
Independent Service Auditor's Report

ACCEDERE

Independent Service Auditor's Report

To: The Management of Cisco Webex Meetings
Location: San Jose, CA, USA

Scope

We have examined Cisco Webex Meetings: Webex Messenger, Webex Meetings, Webex Training, Webex Events, Webex Support, a product of Cisco Collaboration Technology Group (CTG), and the accompanying assertion titled "Cisco Webex Meetings Management Assertion of …" that the controls within design of Cisco Webex Meetings were effective throughout the period October 13, 2017 to October 12, 2018, to provide reasonable assurance that Cisco Webex Meetings commitments and system requirements were achieved based on the trust services principles & criteria (TSPC 2016) relevant to security, availability, confidentiality, and privacy (applicable trust services principles & criteria) set forth in TSPC *2016 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) along with covering Cisco's worldwide applicability of controls of the standard C5 Cloud Controls (Cloud Computing Compliance Controls Catalogue).

Cisco Webex Meetings Responsibilities

Cisco Webex Meetings is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Cisco Webex Meetings service commitments and system requirements were achieved. Cisco Webex Meetings has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Cisco Webex Meetings is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and Cisco's worldwide applicability of controls of the standard C5 Cloud Controls. 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. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Cisco Webex Meetings commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Cisco Webex Meetings commitments and system requirements based on the applicable trust services criteria.
- Cisco Webex Meetings ISO 27001:2013 and 2017:2015 audit conducted by DNV GL and the related evidence

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services principles & criteria and Cisco's worldwide applicability of controls of the standard C5 Cloud Controls. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Cisco Webex Cloud Services were effective throughout the period October 13, 2017 to October 12, 2018, to provide reasonable assurance that Cisco Webex Meetings commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Accedere Inc.
Certified Public Accountants
CPA License No: FRM 5000337
Denver, Colorado, USA
Place of Issue: Denver, CO
Date: October 12, 2018

Stamp & Signature
Ashwin Chaudhary
CPA, CISSP, CISA, CISM, CRISC, CGEIT, CCSK,
ISO 27001 LA, PMP.
info@accedere.us

Annexure to Cisco Webex Meetings SOC 3 Report

October 12, 2018

DNV GL and Accedere Inc. participated in the SOC 3 attestation of Cisco Webex Meetings.

The ISO 27001:2013 and 27017:2015 Audit evidences were shared and used for evaluation of controls which formed the basis for the SOC 3 attestation, to support the applicable criteria for the principles in Trust Services Principles & Criteria (TSPC) 2016 for Security, Availability, Confidentiality, Privacy, and Cisco's worldwide applicability of controls of the standard C5 Cloud Controls.

Shamanna Nandakumar
Lead Auditor, ISMS
DNV GL Business Assurance India Private Limited
Unit No. S2003, 20th Floor, World Trade Center, Brigade Gateway Campus,
No.26/1, Dr. Rajkumar Road, Malleshwaram West, Bengaluru – 560 055
Phone: +91 9845032831
Email: Nandakumar.Shamanna@dnvgl.com
Date: October 12, 2018

Section II
Management Assertion

Cisco Webex Meetings Management Assertion for Webex Messenger, Webex Meetings, Webex Training, Webex Events, Webex Support

We are responsible for designing, implementing, operating, and maintaining effective controls within Cisco Webex Meetings throughout the period October 13, 2017 to October 12, 2018 to provide reasonable assurance that Cisco Webex Meetings commitments and system requirements relevant to security, availability, confidentiality, privacy and the C5 Cloud Controls were achieved. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 13, 2017 to October 12, 2018, to provide reasonable assurance that Cisco Webex Meetings commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSPC 2016 Trust Services Principles & Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) and the C5 Cloud Controls. Cisco Webex Meetings objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 13, 2017 to October 12, 2018 to provide reasonable assurance that Cisco Webex Meetings commitments and system requirements were achieved based on the applicable trust services criteria.

Cisco Systems, Inc.

Section III

Cisco's Description of its

Cisco Webex Meetings: Webex Messenger, Webex Meetings, Webex Training, Webex Events, Webex Support

Report Scope and Purpose

Cisco Webex Meetings product is used in this report to refer to: Webex Messenger, Webex Meetings, Webex Training, Webex Events, Webex Support

This Service Organization Controls (SOC) report is an examination of controls relevant to the security, availability, confidentiality, privacy and the C5 Cloud Controls of the services performed by Cisco Webex Meetings under SSAE 18, Attest Engagements (AICPA, Professional Standards) prepared pursuant to the AICPA guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*.

This section of the report is intended to provide user organizations and independent auditors with information about Cisco Webex Meetings system design and implementation to meet the criteria for the security, confidentiality, and privacy principles set forth, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Principles and Criteria) ("applicable trust services criteria").

Because this description is intended to focus on the controls relevant to achieve the principles *Security, Confidentiality, Availability, and Privacy* only, it does not encompass all aspects of the services or procedures performed by Cisco Systems Inc.

The scope of this report is limited to Cisco Webex Meetings operations including equipment owned by Cisco and operated by permanent, temporary and contract Cisco personnel used for Cisco Webex Meetings operations. Except were specified in the contract operating processes for customers, partners and colocation facilities are beyond the scope of this report.

All policies, process, procedures, monitoring, response, and communication described herein are implemented for the purpose of securing the Cisco Webex Meetings infrastructure and for ensuring the security, confidentiality, and privacy of the all customer information that Cisco Webex Meetings requires to provide the service.

Overview of the Company

Company Background

Cisco Systems, Inc. ("Cisco" or the "Company") (NASDAQ: CSCO) was incorporated in California in December 1984, and is headquartered in San Jose, California. Cisco is a global leader in information technology (IT). Cisco designs, manufactures, and sells Internet Protocol (IP)-based networking and other products related to the communications and IT industry and provides services associated with these products and their use. Cisco provides a broad line of products, services, and solutions for transporting data, voice, and video within buildings, around campuses, and around the world. Cisco products are designed to transform how people connect, communicate, and collaborate. Cisco products are installed at enterprise businesses, public institutions, telecommunications companies and other service providers, commercial businesses, and personal residences.

Collaboration Technology Group

Cisco is organized into business units and corporate functions. The Cisco Webex product is in the business unit called Collaboration Technology Group (CTG). CTG is comprised of a suite of products that make work more intuitive with easy-to-use collaboration technology. The suite of collaboration products enable businesses through Unified Communications, Contact Center, Conferencing, and Collaboration Endpoints solutions.

For more information on Cisco, refer to: https://www.cisco.com

Cisco CTG Webex Security Organization

Security always comes first for Cisco Webex. Everything you share, say, and type is protected by end-to-end encryption. Authorized administrators can manage and enforce security policies. And thanks to Cisco's high security standards, Cisco Webex products are some of the most secure collaboration tools available.

The Cisco Security and Trust Organization is committed to maintaining strong protections for our customers, products and company by being trustworthy, transparent and accountable. The Cisco CTG Webex security organization is part of the Security and Trust Organization and is also embedded in the Cisco Webex product operation. The organizational independence and intrinsic presence institutionalizes security first for Cisco Webex product.

For more information on Cisco's commitment to security, refer to:

https://www.cisco.com/c/en/us/about/trust-center.html

Controls Common for CTG

CTG uses common and shared controls for cloud products in the CTG portfolio. This report describes these common controls and following Controls Common for CTG is the description of the controls that are specific to the Cisco Webex Meeting product.

Compliance and Governance

Management, in conjunction with the groups it creates, is responsible for creating, maintaining, and monitoring the policies, standards, and procedures that constitute the internal controls deemed to provide reasonable assurance of the integrity and reliability of the production systems, and for the protection of customer information and assets against unauthorized use and

disposition. Compliance with Cisco policies and standards is required and verified. Leading the priority and focus on security is the CTG Governance Committee (GC). The GC is comprised of Cisco CTG Webex Security and Cisco Webex product leaders. The GC is accountable for the overall governance framework, planning, directing, and controlling the security and risk aspects of business operations. The GC assigns roles and responsibilities to provide oversight to confirm adequate resourcing, efficiency of operation, and separation of duties. The key roles and responsibilities of the committee are:

- Chief Information Security Officer (CISO) – accountable to information security for Cisco Webex product
- Cisco CTG Security Compliance team – responsible for the governance of Cisco Webex product within the Cisco CTG Webex Security organization. This team is responsible for maintenance of the Information Security Management System (ISMS)
- Security Operations team – responsible for the operations of security compliance such as baseline configuration management and vulnerability management
- Cisco Webex product leadership and team – responsible for the implementation and execution of security processes and procedures

Information Security Management System

Cisco has established and maintains formal policies, standards, and procedures to delineate the standards relevant to the design and operations of controls over the Cisco Webex product. CTG has an Information Security Management System (ISMS) designed to meet ISO/IEC 27001:2013 and 27017:2015 requirements implemented and operating on an annual cycle. Policies are reviewed and approved on a periodic basis, published on the company intranet, and communicated to CTG employees and contractors. Organizational roles, responsibilities, and competency requirements affecting the security, confidentiality, and privacy of the services are defined and assigned by CTG management and communicated to the CTG organization.

The Information Security Policy defines the management commitment to Information Security and the information security program. The policy requires developing processes and procedures to protect security, confidentiality, and privacy of customer data, and to ensure compliance to applicable legal requirements, contractual obligations, and any security requirements. Management is responsible for periodic assessment of the level of compliance to legal requirements, operational controls, and overall risk posture. Assessment reports are presented to the ISMS GC and other appropriate levels of management which include:

- The importance/criticality of information resources
- The effectiveness of present information security arrangements
- Special circumstances that increase the probability of incidents occurring
- New threats and vulnerabilities
- Recommendations for ongoing improvements
- The status of current improvement activities

ISMS processes and procedures including the following govern information technology:

- Access Management
- Asset Management
- Personnel Management

- Change Management
- Configuration Management
- Cisco Secure Development Lifecycle
- Data Center Security (if applicable)
- Incident Management
- Vulnerability Management
- Business Continuity Management

CTG evaluates its organizational structure, reporting lines, authorities, and responsibilities for appropriate scope, competence, and position within the organization on an annual basis as part of its business planning process. CTG monitors global regulatory requirements to ensure relevant statutory, regulatory, and contractual requirements are identified, documented, and kept up to date through regular interaction with legal, operations, and compliance business units.

Internal Communication

The CTG ISMS program uses a variety of mechanisms to communicate security requirements and expectations to its employees and contractors. The following assure that employees and contractors are informed and understand our security policies and expectations:

- Acknowledge the Company Code of Business Conduct (COBC)
- Take and pass the annual Security Awareness training course
- Read the Security Policies and Standards
- Take and pass the Cisco Security Ninja Program

During onboarding and annually thereafter, the organization provides mandatory Annual Security Awareness training which reaffirms the location of all policies and standards. Annually, the Organization Business Unit leader will send an email containing:

- The importance of adhering to the Organization Information Systems Policy
- The importance of meeting the Organization Security Objectives
- The importance of the ISMS
- The importance of adhering to the ISMS
- The Organization's responsibilities under the applicable laws & regulations
- The criticality of continual improvement
- Link to CTG ISMS Standard Manual, which contains:
    1. The latest version of the CTG Information Systems Policy
    2. The latest version of the CTG Security Objectives
    3. Link to ISMS Policies and Standards intranet page
    4. Link to the CTG ISMS Roles and Responsibilities document containing roles, responsibilities, and authorities

The CTG ISMS program maintains resources to communicate internally all ISMS documentation, policies, and standards. These policies and standards are managed in Cisco's enterprise documentation control system. An ISMS GC representative will send an email quarterly to

employees, contractors, consultants, temporaries, and other workers with selected relevant information.

Internal Audit and Risk Management

CTG management is responsible for identifying the risks that threaten the achievement of the control objectives for the Cisco Webex product. The CTG GC meets quarterly to review risks, mitigations, and required actions.

At the direction of CTG GC, an independent group within the Security & Trust Organization performs an Internal Audit at least annually. In addition, the independent group performs a Risk Assessment at least annually. The Internal Audit and Risk Assessment identify risks in the Cisco Webex product. Management then implements appropriate measures to address those risks.

The Internal Audits and Risk Assessments are conducted for the Cisco Webex product production system and operations. If applicable to the Cisco Webex product, an Internal Audit and Risk Assessment will be performed on each data center.

Risk Assessment Methodology

The overall steps of the risk assessment include:

- Plan the risk assessment
- Establish context
- Perform assessment including risk identification, risk analysis, and risk evaluation
- Determine risk treatment options
- Document risk acceptance
- Communicate and consult on risk
- Monitor and review

Risks are analyzed for their possible impact and likelihood, yielding a level of risk determination and corresponding acceptance criteria. Risks are assessed and evaluated both at the global level and the site-specific level. Risk treatment, following the risk assessment, evaluates cost effective controls or measures. Management uses the following risk treatment options to assist in the decision making process of treating residual risks:

- Risk Modification (Mitigate) – The level of risk should be managed by introducing, removing, or altering controls so that the residual risk can be reassessed as being acceptable
- Risk Retention (Accept) – The business unit decides to accept the potential risk and continue operating with the risk. This acceptance is a conscious business decision based on a number of factors such as the organization's culture, risk appetite, and potential opportunity loss
- Risk Avoidance (Terminate) – When the identified risk is considered too high or the cost of implementing treatment options exceeds the benefits, a decision may be made to avoid the risk completely by withdrawing from a planned or existing activity or set of activities or changing the conditions under which the activity is operated
- Risk Sharing (Transfer) – The risk may be treated by transferring the risk using options such as purchasing insurance to compensate for the loss incurred if the risk materializes

Using the above criteria, the risk assessment team combines the evaluated controls with the risk treatment options and provides a risk assessment report to management.

Cisco Secure Development Lifecycle

Cisco Webex product is compliant with the Cisco Secure Development Lifecycle (CSDL).

The combination of tools, processes, and awareness training introduced in all phases of the development lifecycle ensures defense-in-depth, and provides a holistic approach to product resiliency. CSDL is a process to ensure Cisco develops cloud solutions that adhere to the Cisco and industry security standards.

CSDL compliance is calculated based on information provided by the product teams. It is measured based upon compliance to Product Security Baseline (PSB) requirement-level data, and is monitored over time. Compliance with CSDL cannot be waived.

For Cisco cloud products, CSDL for Cloud requires a Cloud Approval to Operate (CATO). The CATO is Cisco's three-phase certification process. First is the discovery phase, where registration and security planning occur. Second is the assessment phase where CSDL PSB requirements are implemented, and attainment of the CATO approval to operate is achieved. The third phase is the governance and maintenance of the CATO on an annual basis.

For more information regarding Cisco's Secure Development Lifecycle, refer to:

https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle.html

Data Privacy & Protection

The S&TO Global Data Privacy Office is responsible for data privacy of Cisco assets. The S&TO Data Protection Program team manages the liability of data privacy of Cisco assets. The GDPO and DPP teams are a service to help product teams examine their products and services to remove any privacy or digital friction, including privacy compliance. Privacy engineering requirements defined by the GDPO team are integrated in the CSDL for Cloud CATO process.

The Cisco Webex product team works with the GDPO and DPP teams to fully understand data privacy. In addition, every Cisco worker and partner is continuously accountable to the protection of customer information.

Policies, procedures, standards, guides, and resources available to enable complete understanding and enforcement of Cisco's data lifecycle include:

- Privacy and Data Protection
- Customer Data Protection
- Security Ninja White Belt (Data Privacy and Security Centric Training)
- Enterprise Records Management Policy
- Enterprise Record Retention Schedule
- Corporate Data Protection Standard
- Corporate Backup Data Retention and Media Rotation Policy
- Legal Services (NDA and queries)

To maintain consistency across the company and drive the appropriate protections for specific categories of data, Cisco has an enterprise-wide Common Data Taxonomy:

- Administrative Data
- Customer Data
- Entrusted Data
- Financing Data
- Telemetry Data
- Support Data
- Cisco Operations Data
- Cisco Strategic Data
- Human Resources Data

Consistent categorization of data allows Cisco to develop category-specific data protection requirements that reflect the company's obligations for such data.

Data Impact Analysis

Every product at Cisco undergoes a complete Data Impact Analysis (DIA). This detailed and multiphase process can be summarized by the following mandatory initial questions:

- What data does your organization collect and or use?
- How is your data processed?
- Who accesses your data?
- Where is your data stored?
- What is the sensitivity, classification, and category of the PII data?
- What is the intended use for collecting this PII and are there other usages for it?
- What is the overall volume of this data, both traversing and in storage?
- What is the criticality of the underlying service or functions being performed by this application?

Cisco implements privacy criteria as a part of its Data Impact Assessment (DIA) and its Privacy Impact Assessment (PIA). Elements that are common in the Cisco taxonomy and the Trust Services Privacy Principle include:

- Notice and communication of commitments and system requirements
- Notice to data subjects about privacy practices, commitments, and system requirements
- Choice and consent. Detail choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects
- Collection minimization
- Use, retention, and disposal; Cisco limits the use, retention, and enforces disposal of PII
- Access. Cisco provides data subjects with access to their personal information for review and correction (including updates) to meet its privacy commitments

Privacy Assessment

- Cisco's offerings (clouds, products) and IT applications must meet customer and regulatory requirements regarding the processing of personal information. Cisco has developed a Privacy Impact Assessment (PIA) process intended to:
- Give relevant privacy guidance to development teams in an efficient and agile way that enables fast, informed decision-making
- Flag potential privacy issues as early as possible in the development cycle

The assessment process applies to all Cisco offerings and IT applications that collect, use, and distribute customer, employee, or 3rd party personal data.

Each assessment contains the following components:

- PIA - General Info - Provides basic information and whether or not personal information is collected, used or distributed
- PIA - Privacy Controls - Section that established what controls the Offering or Application provides to protect privacy data and meet additional regulations
- PIA - Privacy Data Inventory - Inventory of the privacy data elements, including appropriate metadata
- PIA - Supporting Documentation - Area provided to leave more information where necessary
- PIA - Assessment - Final worksheet completed by the Privacy Assessment team

Vulnerability Management

A vulnerability management program, managed by the InfoSec Cloud Security team, is in place to assess vulnerabilities in the Cisco Webex product environment. Assessments are performed on an on-going basis using a vulnerability scanner and penetration testing.

Beginning with an accurate inventory of all assets, the vulnerability management process employs a vulnerability scanning tool to verify the security of the information system and applications. All vulnerabilities found using the scanner and penetration testing are entered into the vulnerability repository where they are evaluated (triaged) and categorized based on severity and their common vulnerability scoring system (CVSS) score. False positives are identified and eliminated. Vulnerabilities are assigned to the responsible team for remediation with a resolution date. After remediation is complete, the environment is scanned to verify that the issue has been resolved.

Penetration Testing

Penetration Testing aims at finding security issues by using the same tools and techniques as an attacker and are used to help secure products and services. A Penetration Test is defined as a legal and authorized attempt to find and successfully exploit systems, products, and services for the purpose of making them secure. Penetration Testing goes a step beyond vulnerability assessment by simulating hacker activity and delivering a live payload. Proof of Concept (PoC) attacks demonstrate that the capability to exploit is real.

Independent third-party Network Penetration Tests are performed annually. The results of this testing are made available upon request. Additionally, component based Penetration Tests of the Cisco Webex product occurs when there are significant changes. All results from Penetration Tests are managed and analyzed for improvements in the Vulnerability Management process.

Product Security Incident Management

Cisco has established policy that defines the roles and responsibilities of management for handling suspected data breach, data loss, and computer security incidents at Cisco. This policy defines requirements and procedures for incident detection, reporting, and response. Cisco has response teams that will respond to security incidents 24 hours a day, seven days a week.

The incident management process defines which employees, contractors, and third-parties to contact in case of an incident or awareness of a security weakness. It also defines the systematic steps in which the product security team responds to a security incident including, but not limited to, the identification and validation of an incident, damage control or remediation, service restoration, evidence collection and preservation, contact with authorities, and post-mortem evaluations.

The product security incident management team is responsible for:

- Identifying and reporting suspicious activity
- Monitoring and handling incidents that originate from intrusion detection/prevention systems and other perimeter monitoring devices
- Executing the Security Incident Response Management process
- Performing Incident Response Testing
- Performing Incident Response Training
- Notifying customers

Incident Monitoring

Cisco Webex product employs multiple technologies, procedures, and teams to ensure secure operation. Cisco has implemented key operational metrics and alarms across the production network using a variety of automated monitoring systems to detect outages, service latency, security incidents, and other unusual or unauthorized activities and conditions. Alarms are configured to notify operational and management personnel when warning thresholds indicating potential service latency, server unavailability, or other factors affecting availability and functionality are breached. Personnel are on-call at all times to ensure that alarms are responded to in a timely manner.

Incidents and threshold warnings are logged in the incident tracking system. They are assigned a priority level and ownership and tracked through to appropriate resolution.

A key prerequisite for incident monitoring and response is event logging and centralized logs. Cisco has established a *policy* that defines the requirements for logging data at Cisco. This policy establishes requirements for event types, time synchronization, content and other key information. Logs are centralized for aggregation, correlation, continuity, and retention.

Incident Response

The Cisco Product Security Incident Response Team (PSIRT) is responsible for responding to Cisco product security incidents. The Computer Security Incident Response Team (CSIRT) provides proactive threat analysis, incident detection, and internally coordinated incident response. In addition, the Cisco Webex product team monitors and responds to security incidents in coordination with PSIRT and CSIRT.

Cisco Product Security Incident Response Team (PSIRT)

The Cisco Product Security Incident Response Team (PSIRT) is responsible for responding to Cisco product security incidents. The Cisco PSIRT is a dedicated, global team that manages the

receipt, investigation, and public reporting of information about security vulnerabilities and issues related to Cisco products and networks. Cisco defines a security vulnerability as an unintended weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of the product. The Cisco PSIRT adheres to ISO/IEC 29147:2014

The on-call Cisco PSIRT works 24 hours a day with Cisco customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security vulnerabilities and issues with Cisco products and networks.

The following are the steps in the Cisco Product Security Incident Response Process:

- Awareness: PSIRT receives notification of security incident
- Active Management: PSIRT prioritizes and identifies resources
- Fix Determined: PSIRT coordinates fix and impact assessment
- Communication Plan: PSIRT sets timeframe and notification format
- Integration and Mitigation: PSIRT engages experts and executives
- Notification: PSIRT notifies all customers simultaneously
- Feedback: PSIRT incorporates feedback from customers and Cisco internal input

The Cisco PSIRT investigates all reports regardless of the Cisco software code version or product lifecycle status. Issues will be prioritized based on the potential severity of the vulnerability and other environmental factors. Ultimately, the resolution of a reported incident may require upgrades to products that are under active support from Cisco.

Throughout the investigative process, the Cisco PSIRT strives to work collaboratively with the source of the report (incident reporter) to confirm the nature of the vulnerability, gather required technical information, and ascertain appropriate remedial action. When the initial investigation is complete, results will be delivered to the incident reporter along with a plan for resolution and public disclosure. If the incident reporter disagrees with the conclusion, the Cisco PSIRT will make every effort to address those concerns.

Cisco has published a Security Vulnerability Policy that describes:

- How to report or obtain support for a suspected security vulnerability
- Details on the incident response process
- Communications and disclosure plans

For more information on the Security Vulnerability Policy, refer to:

https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html

For more information on Cisco Security Advisories and Alerts, refer to:

https://tools.cisco.com/security/center/publicationListing.x

https://www.cisco.com/c/dam/en_us/about/security/psirt/Cisco-PSIRT-Infographic.pdf

https://tools.cisco.com/security/center/emergency.x?i=56

Cisco Computer Security Incident Response Team (CSIRT)

Cisco CSIRT forms part of the investigative branch of the Cisco Security and Trust Organization (S&TO), and provides proactive threat analysis, incident detection, and coordinated incident response. The primary mission of Cisco CSIRT is to review security architecture, establish incident management procedures for collecting incident data, enable efficient recovery from

security incidents, prevent or minimize disruption of critical computing services, and facilitate cooperation and information exchange among cross-functional groups that are responsible for security incident remediation. Cisco CSIRT helps protect Cisco employees, business partners, and Cisco-owned businesses.

Cisco CSIRT is a global team of analysts, investigators, and engineers that serve the IT, business, and engineering organizations within Cisco, and more specifically, the Chief Security Officer (CSO) and the company senior management team, to help protect Cisco information assets. Cisco CSIRT coordinates, investigates, and remediates security incidents, and its investigators provide forensic investigations support at the direction of the Cisco CSO, and within the framework defined by Cisco HR, Cisco Legal, and external entities, including law enforcement.

S&TO has developed an Incident Response Plan which provides a high-level approach for how the incident response capability fits into the overall organization and describes the structure and organization of the incident response capabilities.

The incident handling methodology consists of the following phases:

- Incident Preparation
- Incident Detection and Analysis
- Incident Containment, Eradication, and Recovery
- Post Incident Activity and Evidence Collection

All incidents are considered normal priority unless they are labeled EMERGENCY. All incoming information is handled confidentially by Cisco CSIRT, regardless of its priority. Cisco CSIRT supports the Information Sharing Traffic Light Protocol (ISTLP). Information that arrives with the tags WHITE, GREEN, AMBER, or RED will be handled appropriately.

For more information on ISTLP, refer to: https://www.first.org/tlp/docs/tlp-v1.pdf

Cisco CSIRT collaborates with FIRST, the National Safety Information Exchange (NSIE), the Defense Security Information Exchange (DSIE), and the DNS Operations Analysis and Research Center (DNS-OARC).

External and internal users can make reports to CSIRT by submitting an incident reporting email notification to Cisco CSIRT management and investigators team email address: csirt-notify@cisco.com.

For more information on the Cisco CSIRT RFC 2350 Profile, refer to:

https://www.cisco.com/c/en/us/about/security-center/computer-security-incident-response-team-csirt.html

Reporting a Data Incident

Cisco has a Data Protection Program Incident Response Team that responds to possible data incidents 24 hours a day, seven days a week. Cisco provides a data incident reporting tool. Once a new incident is submitted, a Data Protection Incident Investigator is assigned and reviews the Incident. The following steps are taken in response to the data incident submitted:

- Investigation: After the new incident is created, CSIRT & DPP incident investigators evaluate the incident to better understand the impact. Once confirmed as a data incident requiring escalation, the DPP Incident Response Team is assembled to:
    1. Review the incident
    2. Develop a response plan

3. Resolve the incident with the data protection specialists from the impacted organization

- Remediation: The Incident Commander is the leader of the resolution efforts to ensure that both the Root Cause and Corrective Actions are identified. This results in the Incident Response team working cross company to ensure appropriate actions by the impacted organization. The Cisco Data Protection team responds to data issues promptly, however we are committed to creating a culture of data protection. Mistakes do not result in reprimand and prompt recognition and reporting is advocated. The best chance of minimizing a data handling error is though quick recognition and engagement of the Data Protection team.
- Communication & Awareness: Incident Commander is responsible for ensuring all relevant and interested parties are aware of the situation. They will brief both the Cisco executive and functional staffs as appropriate. Other responsibilities of the Incident Commander include:

    1. Document response learnings
    2. Create training materials where appropriate
    3. Roll out materials and new practices with the Incident Investigator

Supplier Management

Cisco's Supplier Management program begins with the corporate controls governing the procurement organization. Suppliers enter into an agreement which covers supplier duties, services, license and intellectual property rights, confidentiality, integrity, and availability. Suppliers are required to report information security events. Agreements include security requirements and Service Level Agreements.

After complying with the corporate procurement process, products' key suppliers are subject to annual reviews. These cover the handling of non-public information, legal review, budget for the previous and next year, the security of the system, external certifications, as well as pertinent organizational structure reviews if they will affect the stability of the vendor.

If a supplier is a cloud service provider the product team must ensure that this product is evaluated by Cisco's third party security assessment program. This program is the CASPR/CASPRX process. CASPR/CASPRX assessments evaluate the security risks to Cisco from use of a supplier's product or service, and provide recommendations. The benefits include validation of the supplier's security architecture for compliance with Cisco policies and standards, a proactive and predictable process, and the protection of Cisco data and brand.

Personnel Management

Cisco human resource policies, procedures, and guidelines apply to all Cisco permanent, temporary, and contract personnel. Personnel management requirements include background checks, Code of Business Conduct review, and education and training.

Cisco requires that newly hired employees certify that they have reviewed, understand, and agree to confidentiality and data protection policies and guidelines by signing the Code of Business Conduct (COBC). Contractor companies are required to sign a contract including terms and conditions with confidentiality and non-disclosure restrictions.

The confidentiality policies and restrictions identify and address the following:

- Requirement to protect confidential company, former employer, and third party information and inventions
- Duration of coverage
- Terms for information to be returned or destroyed at contract cessation
- Expected actions to be taken in case of a breach of the contract or policies

Background Checks

Background checks are conducted on anyone who requires badge access to Cisco facilities, electronic access (email, intranet access, etc.), or any access to Cisco's confidential, proprietary or intellectual data. This includes pre-employment background investigations on all Cisco employees, and pre-access background investigations on all non-employees (temporary workers, contractors, consultants, vendors, and access-only individuals).

Anyone receiving access to Cisco facilities, systems, or sensitive information must meet Cisco's background check standards. Any applicant who refuses to complete the background check process will not be eligible for Cisco employment or Cisco access. Cisco complies with all applicable federal, state, and local laws, including fair employment practices and equal employment opportunity, when conducting background checks. All pre-employment and pre-access background checks are individually assessed.

Pre-access background checks for non-employees

Pre-access background checks must be conducted on any non-employee (temporary worker, contractor, consultant, vendor or access-only individual) who requires badge access to Cisco facilities, electronic access (email, intranet access, etc.), or any access to Cisco's confidential, proprietary or intellectual data. The Supplier is responsible for initiating the background check with one of Cisco's preferred background screening vendors and assumes all costs incurred in the background screening process. Cisco does not initiate nor complete background checks for non-employees. Background checks must be completed no earlier than 6 months prior to the non-employee's start date.

Nondisclosure Agreement

All Cisco employees, vendors, and contractors who require access to Cisco facilities, systems, or sensitive information are required to sign a confidentiality and a nondisclosure agreement (NDA) before being granted access.

Additionally, the Cisco Acceptable Use Policy describes user responsibilities and establishes expected behavior when using all of Cisco systems, devices, application, and services (including cloud services). All users, including employees, vendors, and contractors are required to follow the rules of behavior. The agreements are put in place to protect trade secrets, sensitive, and business confidential information and assets.

The NDA includes statements regarding information and asset protection responsibilities. They also describe the penalties for the violation of these responsibilities. Additionally communicated is the fact that the user's security responsibilities extend outside of the work site, beyond the standard operating hours of their employment and continue for a defined period after employment ends. Signed confirmation from users indicating understanding and agreement is required prior to their gaining access to Cisco facilities, systems, or sensitive information.

Code of Business Conduct

Cisco requires all employees to certify annually that they have reviewed, understood, and agreed to the confidentiality and data protection policies and guidelines as set forth in the Cisco Code of

Business Conduct (COBC). The COBC sets guiding principles governing Cisco personnel behavior with respect to ethics, legal compliance, safeguarding proprietary and confidential information, conflicts of interest and other relevant areas. New hires are required to review and acknowledge the Cisco Code of Business Conduct. Contractors are required to review and agree to a confidentiality agreement with their employer as a condition of working at Cisco.

Education and Training

Cisco requires all permanent, temporary and contract personnel to take the following education and training, as applicable, in support of external security certifications:

- Security Awareness Training – This is annual training prepared by Cisco's Data Protection and Privacy team which features different security topics each year. All applicable personnel are required to take this training annually
- Cisco Ninja White Belt Training – This is one-time training on security fundamentals. All applicable personnel are required to complete this training

Overview of Cisco Webex Meetings

Cisco Webex Meetings Organization

Cisco Webex Meetings is part of the Cisco Collaboration Technology Group (CTG). The following are the roles accountable to the security, availability, confidentiality, privacy, and the C5 Cloud Controls:

- Vice President and General Manager
- Director of Engineering
- Director of Operations
- Director of Product Management

These roles are responsible for working with the Cisco CTG Webex Security team and the Security and Trust Organization (S&TO) where there is a shared responsibility and governance for Cisco Webex Meetings.

Cisco Webex Meetings Product Overview

Cisco Webex Meetings is a cloud-based service that provides virtual meeting rooms in which participants from diverse locations can collaborate in real time. The core of the Cisco Webex Meetings offering is to host audio and video conferencing with data sharing, and chat.

Cisco Webex Meetings offers its customers several types of conference services through ISPs and partners. These services provide different conference formats correspondent with customer needs. Services include the following:

- **Webex Meetings** – Webex Meetings is a Web and Video Conferencing that enables people to easily meet, collaborate, and stay productive anywhere, anytime, on any device
- **Cisco Collaboration Meeting Rooms Cloud –** Collaboration Meeting Rooms (CMR) is a video conferencing feature in the Webex Meetings subscription from the Cisco Collaboration Cloud
- **Webex Cloud Connected Audio –** Cloud Connected Audio (CCA) is an enterprise audio conferencing solution for Webex meetings that extends IP Telephony
- **Webex Events** – Webex Events makes it easy and cost-effective to enhance user's reach and effectiveness with online events and meetings. Users can communicate with internal and external audiences on a larger scale. Speakers can also interact with participants in real time using polling, chat, and threaded questions and answers (Q&A)
- **Webex Training** – Webex Training is a hosted online training solution that makes it easy to deliver highly effective, live instruction - to anyone, anywhere
- **Webex Support** (including Webex Remote Access) – Webex Support provides real-time IT support and customer service to employees and customers anywhere in the world
- **Webex Messenger** – Webex Messenger delivers Enterprise Instant Messaging (EIM) services securely over the Internet

Cisco Webex Meetings are installed on computer clusters located in data centers distributed around the world. Each service cluster in the data center connects to the larger Cisco Webex Meetings network which provides configuration, conference management, and security. The Cisco Webex Meetings network for each cluster connects to the Cisco network which provides additional security and separation for the Cisco Webex Meetings production environment.

System and Boundary Definition

The Cisco Webex Meetings Network illustrated in Figure 1, represents the traffic flow from the customers and Cisco Webex Meetings administrative personnel into the Cisco Webex data center.

Customer traffic originating on a Cisco Webex Meetings client is encrypted on the device and is carried across the internet to the Cisco data center. At the data center, customer traffic enters the Cisco shared network and is routed to the Cisco Webex Meetings network environment. Cisco Webex Meetings network border implements security through firewalls, intrusion detection systems (IDS), SSL load balancers, and SSL accelerators before it is handed off to the next architecture layer for processing. The SSL accelerator terminates the session preventing direct connection between the user and the Cisco Webex Meetings environment. Firewalls are installed between all Cisco Webex Meetings production network segments.

Cisco Webex Meetings administrative traffic follows in a similar course as customer traffic. Cisco Webex Meetings administration is segmented by function. Administration is role-based such that an administrator access approval is granted to a specific function in the network. (See Access Management)

Cisco telecommunications and networking uses various mechanisms, devices, software, and protocols across interrelated and integrated programs designed to protect its customers and its data.

Cisco Webex Meetings uses a wide spectrum of intrusion detection system (IDS), varying from devices to software applications that monitors the network systems for malicious activity or policy violations.

Cisco Webex Meetings network infrastructure components add protection between Cisco Webex Meetings production components and external and internal users. The network perimeter is protected by firewalls. Any network traffic entering or leaving the Cisco Webex data center is continuously monitored using an intrusion detection system (IDS). The Cisco Webex network is also segmented into separate security zones. Traffic between the zones is controlled by firewalls and access control lists (ACLs).

Key infrastructure components include the following:

- **Firewalls –** Filter traffic through Cisco Access Control Lists (ACL). ACL filters ensure that only traffic from approved source IP addresses are allowed
- **IDS –** Intrusion detection systems are used to analyze unencrypted traffic and identify known attacks and abnormal behavior. The appropriate security personnel are alerted when incidents are detected
- **SSL Load Balancers –** Distributes SSL-based traffic among Cisco Webex Meetings application processors
- **SSL Accelerator –** Negotiates SSL connection with Cisco Webex Meetings application processors. Terminates traffic
- Core Cisco Webex Meetings production components include the following:
- **Application and Web Servers** – provide authentication of customer users and site administration; Meeting portals for scheduling, editing, and attending meetings; and static content for pages. Customers are displayed a different Cisco Webex Meetings landing page based on privileges assigned to the user

- **Meeting Server** – provides desktop sharing capability for customer users. Desktop sharing includes remote desktop meetings, sharing of applications, and sharing of the desktop
- **Multimedia Server –** enables VOIP and video conference capability for customer users. When meeting attendees choose this option, voice conferencing is performed within the application and leverages a user's laptop speakers and microphone or a connected headset
- **Telephony Server** –provides audio conferencing service and serves as an audio bridge for PSTN and IP telephony devices. This option provides a phone number, meeting number and security PIN that users may dial into a meeting integrated with the Webex application hosted on a users' browser

Internal Cisco Webex Meetings users perform a variety of functions for Cisco Webex operations. Management Layer section in the drawing indicates functions internal users are subject to, manage, or apply in the Cisco Webex Meetings environment. An overview of the functions is as follows:

- **Authentication** – Cisco Webex Meetings uses several types of authentication methods to manage access to all parts of the production environment. Privilege levels have been created to manage internal user access to different aspects of the network and customer access to the service
- **Database** – Database servers are used to store configuration, meeting metadata, and meeting recordings when they are requested
- **Application** – The application server supports activity that includes authentication of customer users, site administration, and the meeting portal for scheduling, editing, and attending meetings
- **Security** – Security tools are used to monitor the network, identify risk, collect data, store data, and analyze data

Customer Data Flow

Cisco Webex Meetings defines three, core user roles pertinent to the flow of customer data in the system: site administrator, host, and attendee. The site administrator is responsible for managing the customer's Cisco Webex Meetings site including its configuration and creating hosts. A host is an end user to whom the site admin grants permission to create a Cisco Webex meeting. Attendees are meeting participants who may or may not be configured users. Customer data in the system takes two forms: configuration data including personal data that is used for establishing connections and conference data which can include voice and video, shared applications such as spreadsheets, white board, chat, etc. Figure 2 shows how customer data flows in the Cisco Webex Meetings environment.

Site Administration Flow

Once a customer has designated a person to perform the site administration role, Cisco Webex Meetings provides that person appropriate credentials to access the Cisco Webex Meetings portal to the customer's site. The person uses the information provided to access the portal, then configures the customer's site including creating users and uploading a certificate for authentication. The configuration information is stored in the Web zone shown in Figure 2.

Cisco Entity Controls

Overview of Controls

The AICPA deems internal controls as processes that are developed and implemented by an entity's board of directors, management, and other personnel designed to provide reasonable assurance of achieving the entities objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

The AICPA further identifies five interrelated components in which to view these categories:

- **Control Environment** – The overarching tone of the organization affecting the control consciousness of its people. This is the foundation for all other components of internal control providing discipline and structure
- **Control Activities** – Policies and procedures that are established and executed to ensure that the actions identified by management as necessary to address risks to achieve the entity's control objectives are effectively carried out
- **Information and Communication** – Systems, both automated and manual, that are used to identify, capture and exchange information that allow entity personnel to carry out their responsibilities
- **Monitoring** – The process of assessing the quality and effectiveness of the internal controls over time
- **Risk Management** – The processes the entity uses to identify and analyze the risks to achieving its objectives that are the basis for determining how the risks are managed

Cisco Webex Data Protection

Cisco takes customer data protection seriously and it collects, uses, and processes customer information only in accordance with the *"Cisco Privacy Statement"*.

The Cisco Webex (SaaS) Terms of Service provides additional information: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/universal-cloud-agreement.pdf

Several layers of security technologies and processes protect all data collected in Cisco Webex Meetings. Below are examples of controls placed in different layers of Cisco Webex Meetings operations to protect customer data.

- **Physical access control** – Physical access is controlled through biometrics, badges, and video surveillance. Access to the data center requires approvals and is managed through an electronic ticketing system
- **Network access control** – The Cisco Webex Meetings network perimeter is protected by firewalls. Any network traffic entering or leaving the Cisco data center is continuously monitored using an intrusion detection system (IDS). The Cisco Webex Meetings network is also segmented into separate security zones. Traffic between the zones is controlled by firewalls and access control lists (ACLs)

- **Infrastructure monitoring and management controls** – Every component of infrastructure, including network devices, application servers, databases, and storage devices, is hardened to stringent guidelines. They are also subject to regular scans to identify and address any security concerns
- **Logical access control** – All access to systems is allowed only in accordance with the "segregation of duties" principle. It is granted only on a need-to-know basis and with only the level of access required to do the job. Employee and contractor access to these systems is regularly reviewed for compliance. Cisco employees and contractors do not access customer data unless access is requested by the customer for support reasons
- **Data Retention -** A custom retention period is set for Cisco Webex meetings. Customer Active Site Data is stored as long as that site is active, until the customer requests deletion. Customer deactivated Sites will hold the data for 6 months and after that it will be purged. Customer User Meeting Data will be stored in the database for 13 months. All data containing large meeting tables are partitioned and are kept for 13 months and then the partitions are deleted. After the retention period is reached, all the content is purged and becomes irretrievable.

With the exception of CMR enabled devices, all data in-transit to and from the Cisco Webex data center to Cisco Webex Meetings clients is encrypted. Additionally, in accordance with Cisco Cryptographic Key Management standard, passwords are encrypted.

External Communications

Cisco Webex has implemented various methods of external communication to support its customer base and the community. Communication is in place and can be found at the following:

- Operational issues, concerns, or questions: https://collaborationhelp.cisco.com
- Security White Papers: https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/Webex-meeting-center/white-paper-c11-737588.pdf
- Vulnerabilities from PSIRT: https://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html
- Privacy Statement and Supplements: https://www.cisco.com/web/siteassets/legal/privacy_full.html
- https://www.cisco.com/c/en/us/about/legal/privacy-full/Webex-meeting-center-supplement.html
- https://www.cisco.com/c/en/us/about/legal/privacy-full/Webex-messenger-supplement.html
- Cisco Webex (SaaS) Terms of Service to customers, external users, and partners: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/universal-cloud-agreement.pdf
- Webex Configuration and System guides: https://www.cisco.com/c/en/us/support/conferencing/Webex-meeting-center/products-installation-and-configuration-guides-list.html

Cisco Webex Meetings Platform Controls

Infrastructure and Platform Security

Platform security encompasses the security of the network, systems, and the overall data center within Cisco Webex Meetings. All systems undergo a security review and an acceptance validation prior to production deployment.

Firewalls protect the network perimeter and firewalls. Access control lists (ACLs) segregate the different security zones. There are daily internal and external security scans of Cisco Webex Meetings. All systems are hardened and patched as part of the regular maintenance. Additionally, vulnerability scanning and assessments are performed continuously.

All access to network security and management tools is in accordance with Cisco Systems, Inc. Access Management Policy and restricted only to authorized support personnel.

Access Management

Authorization from designated organization officials, including human resources is required before Cisco Systems, Inc. user is provided with a Cisco Corporate Intranet account as part of the employee onboarding process. This provides the user access to the Cisco Corporate Intranet including email.

Internal Users:

Internal users are Cisco Webex employees or contractors having access to Cisco Webex production system. Internal users needing privileged access to Cisco Webex Meetings must request access. The request to create, modify, or delete a privileged user account must come from the user themselves, the employee's HR designated manager or supervisor. The requestor must submit a ticket through a sanctioned workflow management system.

Cisco Webex manages access for internal users via established requirements for administrative access to data and systems (devices, applications, and services) and proper controls for authentication, authorization, and auditing.

Access is role-based; users are granted access via a functional security group. To gain access, an internal user must have a Cisco account and a management authorized ticket must be submitted for any privileged user access.

Termination procedure ensures that the user's credentials are disabled on the day and at the time of termination.

User access rights are reviewed at a minimum of four times annually during the formal RBAC review. This process confirms that managers have adequately modified rights based on role changes within the organization, confirms that no terminated credentials exist in access groups, and validates completeness in the HR termination and management notification procedures. Any issue found would be remediated immediately. Formal changes to roles include notice to appropriate management.

Cisco CTG internal users must use a Cisco issued laptop to access the corporate network and the Cisco Webex environment.

Cisco Webex Meetings Site Administration:

After customer sign up, Cisco Webex Meetings grants the customer permission for a site administrator.

Cisco Webex Meetings requires an administrator to manage the customer's Cisco Webex Meetings site. It has created the site administrator role to fulfill this function. The customer is required to designate and register a site administrator who is then granted privilege to access the Cisco Webex Meetings portal and manage the customer's site. The customer is responsible authenticating and authorizing the site administrator.

The site administrator is responsible for managing the customer's account, enforcing the customer's own policies, and enforcing Cisco Systems, Inc.'s policies and end user agreements. The site administrator creates user accounts and sets user privilege in accordance with the customer's policies and practices. In addition, the site administrator manages the security configuration for their site.

Asset Management

Cisco builds or offers cloud-based services for customers or partners, whether hosted inside or outside of Cisco, including but not limited to Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS). All hosted services environments are subject, regardless of production or non-production.

Cisco's Asset Management applies to the audit and assessment of information, electronic and computing devices (physical and virtual), and network resources used to conduct Cisco business or interact with internal networks and business systems, whether owned or leased by Cisco, the employee, or a third party.

Cisco maintain sufficient processes and documentation necessary to provide current inventory information of system assets.

These assets are: but not limited to:

- **Information Assets:** databases and data files, CA Certificates, contracts and agreements, system documentation research information, user manuals, training material, operational or support procedures, business continuity plans, audit trails, process and risk assessments, and archived information.
- **Software Assets:** application software, system software, development tools, and utilities
- **Physical Assets:** computer equipment, communications equipment, removable media, and other equipment
- **Services:** computing and communications services, general utilities (mostly related to data center environmental facilities)
- **Virtual Infrastructure** (Virtual Machines)

All assets are protected from threats based on a risk assessment.

Change Management

The Cisco Webex Meetings Team manages all aspects of changes to Cisco Webex Meetings. This includes that each change is tested, approved, and reviewed to assure continued function in accordance with platform specifications.

Change requests are logged, categorized, and prioritized according to a formal change management process. Responsibilities are assigned to ensure the proper segregation of duties for the initiation, review, approval, and implementation of change requests. In cases of emergency, any deviation from standard procedures is reviewed by appropriate levels of management, logged,

implemented, and subsequently reviewed, and approved. Emergency change is evaluated as a part of the CAB (change advisory board).

New approved systems or enhancements are forwarded to the Cisco Webex Meetings operations team for migration into production.

Change approval process is restricted to a workflow management system. Only authenticated and authorized users can respond to approval requests. Review of a planned change includes examination of the MOP (method of procedure). The MOP includes the install plan, work details, verification, back-out, and post-implementation review procedures. Engineering will not implement a production change until all approvals are registered in the system. The new systems or enhancements are tested in a pre-production environment and are released in phases to production. Additionally, all changes include a back-out plan. If changes do not meet the agreed quality checks, the engineer will roll back the change. A failed change is required to restart the approval process.

All migration is monitored and issues are escalated up through the various level of technical support. A team of infrastructure engineers and technical operations personnel is assembled to troubleshoot the issue. At the point when change is scheduled, notifications to the end-users inform stakeholders of planned system downtime and any potential impacts due to the change.

Cisco Webex uses policy-enforced maintenance windows to restrict changes in the production environment to a defined timeframe. All changes to the production environment that are outside of the maintenance window require emergency change escalation and approval.

Configuration Management

Cisco Webex Meetings utilizes secure baseline configurations on systems and servers. The baseline configuration is based upon the most current Center for Internet Security (CIS) Benchmark and represents the organization's minimum-security baseline for the technology specific secure installation and configuration of systems, a.k.a., the "hardened image". These hardened images follow the general rule of least functionality where ports, services, and default accounts are only used if required. Recorded as the annual baseline, these configuration plans are formally reviewed and approved as part of annual policy and procedure review.

In situations where the secure host baseline requires an out of cycle configuration change, updated hardened images are pushed to the production environment and undergo routine change management procedures. Operating systems, key components, and network devices are evaluated periodically to ensure conformance with the configuration baseline. Out-of-conformance items are identified and the item is re-provisioned.

Secure Design

Cryptography – Encryption at Run Time

All communications between Cisco Webex Client and Cisco Webex Meetings occur over encrypted channels. Reviewed and approved annually, the Cryptographic Controls Policy and the Cryptographic Implementation Standard ensure the types and levels of encryption necessary for all products and services. This can include password hashing, password encryption, key encryption, file encryption, data at rest encryption, data going over the wire encryption, and configuration file encryption.

Cisco implements transport link encryption for all service end-points. Well implemented encryption is a primary protection for sensitive data, and through proper use, provides greater levels of confidentiality, integrity, and accountability. Transferring data over public or internal

networks must be secured using cryptographic measures such as the Transport Layer Security (TLS) protocol. All customer data being transported over public networks between service end-point and client end device and/or between service end-points must be encrypted at all times. This includes encryption of all customer data being transported via leased lines (e.g. link between data centers using Service Provider).

Cisco Webex Meetings uses Transport Layer Security (TLS) TLS 1.2 protocol and supports all currently registered TLS versions from TLS 1.1 onward. Less secure protocols are disabled by default. Cisco only uses high-strength ciphers (for example, Advanced Encryption Standard (AES) 256). A Product Security Baseline of approved cryptographic primitives represents a mandatory requirement defining the authorized primitives and protocol options for all Cisco offerings (products and services).

For web applications, this encryption requirement also dictates that all communication will be over TLS protocol, including the login page and all subsequent authenticated pages. Implemented encryption must comply with Cisco's minimum encryption algorithm and cryptographic requirements. Media streams flowing from a client to Cisco Webex Meetings servers can only be decrypted after they cross the firewalls inside the Cisco Webex Meetings Data Center systems.

All forms of authentication, cryptographic or otherwise, must demonstrate a reliable trust anchor across their entire trust chain. Cisco enforces that X.509 certificates come from qualified CA's, include only approved certificate authorities, properly generate and present certificates, and restrict certificates to reasonable validity periods through support of certificate revocation, OCSP, and OCSP stapling.

Webex Meetings are established over TLS, with the initial key exchange happening on a TLS-secured channel. All subsequent media streams (audio Voice over Internet Protocol (VOIP), video, screen share, and document share) are encrypted. User Datagram Protocol (UDP) is the preferred protocol for transmitting media. In UDP, media packets are encrypted using AES 128. Additionally, each datagram uses hash-based message authentication code (HMAC) for authentication and integrity. VOIP protocols adhere to H.235 Annex G for SRTP keying/setup with H.323, enforce use of SCCP keying/setup for SRTP with SCCP, DTLS-SRTP for unicast streams, and offer SRTP for all RTP functions.

Data Center Security

Cisco Webex Meetings uses switching equipment located in multiple data centers around the world. These data centers are strategically placed near major Internet access points and use dedicated high-bandwidth fiber to route traffic around the globe. The entire infrastructure within Cisco Webex Meetings is built with industry-standard enterprise security.

Additionally, Cisco Webex Meetings operates network point-of- presence (iPoP) locations that facilitate backbone connections, Internet peering, global site backup, and caching technologies to enhance performance and availability for end users.

Cisco Systems Inc. owns and manages data centers in Mountain View, California and in Richardson and Allen, TX. All other data centers are owned and operated by other external third party owned hosting provider companies.

Cisco Webex CTG monitors the effectiveness of internal control at the external third party owned data centers through regular internal and external audits and risk assessments of data center hosting operations and other procedures.

Cisco Systems, Inc. has established standards and requirements to prevent unauthorized physical access, compromise, theft, or damage information processing facilities and to protect equipment and people against man-made or natural environmental hazards.

Annually, during the risk assessments and annual audit of each data center, ISO 270001 certifications and SOC2 Type II attestation reports are required to complete supplier management activities.

The Cisco Webex Meetings data centers in-scope for this report:

Cisco-owned Data Center

- Mountain View, CA SJC02
- Richardson, TX, USA DFW01
- Allen, TX, USA DFW02

Colocation iPoP Data Centers

- San Jose, CA, USA (Equinix) SJC03
- Sydney, Australia (Equinix) SYD10
- Amsterdam, The Netherlands (Equinix) AMS10
- New York, USA (Telx) JFK10
- Chicago, USA (Telx) ORD10
- Los Angeles, CA, USA (CoreSite) LAX10
- Hong Kong (Pacnet) HKG10
- Dallas, TX, USA (Equinix) DFW10

Colocation Data Centers

- Ashburn, VA, USA (Equinix) IAD02
- Ashburn, VA, USA (Equinix) IAD03
- Tokyo, Japan (Equinix) NRT02
- Toronto, Canada (Equinix) YYZ01
- Singapore (Equinix) SIN01
- London 5, UK (Telehouse) LHR03
- Bangalore, India (Airtel) BLR03
- Almere, The Netherlands (Getronics) AMS01
- Tokyo, Japan (Equinix) NRT03
- Beijing, China (21ViaNet) PEK02

Physical security applies equally to Cisco Systems, Inc.'s hosted facilities and any other external hosting provider.

Physical security at the data center includes video surveillance for facilities and buildings and enforced two-factor identification for entry. Within Cisco Systems, Inc. Data centers, access is controlled through a combination of badge readers and biometric controls. Within the data centers are also "trust zones," or segmented access to equipment based on infrastructure sensitivity. For example, databases are "caged", the network infrastructure has dedicated rooms, and locked racks. Only Cisco Systems Inc. security personnel and authorized visitors accompanied by Cisco Systems Inc. personnel can enter the data centers.

Business Continuity Management

Cisco CTG organization has a formal business continuity plan (BCP) in place. The BCP establishes a process for responding to a catastrophic events. In some cases, the BCP can be relied upon in response to extended disruption of service as laid out in Cisco Systems, Inc. incident response plan (see also, Incident Response). The BCP describes the objectives, assumptions, responsibilities, and actions to be performed in such an event. The plan identifies teams, contacts, responsibilities, and action plans. Planning for the BCP begins with Business Impact Analysis (BIA). The plan is distributed to the Business Functional Team members, Functional Event Program Coordinator, the BCP Champion and Owner and any BCP Team Leads.

Global Site Backup Overview

The Cisco Webex Meetings Global Site Backup (GSB) system ensures that you experience business continuation even in a disaster situation. Additional benefits include full redundancy for maintenance windows or other system outages. GSB provides each customer with a backup site. The GSB system provides real-time, two-way database data synchronization between the primary site and the backup site. All customers are supported with GSB.

A backup site is a separate site from the primary site. Cisco Webex Meetings hosts the backup site on a different system and at a separate geographic location from the primary site.

Automatic Redirection

The GSB system automatically redirects you to your backup site in the event of the entire meeting system failure. If you started a meeting on your primary site and your primary site fails due to a whole system failure, you are automatically routed to the same scheduled meeting on your backup site.

- More information can be found at: https://collaborationhelp.cisco.com/article/en-us/31k2xo

Incident Management

Information Security Incident Management

Cisco has established the *Global Data and Computer Security Incident Management Policy* that defines the roles and responsibilities of management for handling suspected and actual data breach, data loss, and computer security incidents at Cisco. This policy establishes requirements and procedures for incident detection, reporting, and response.

Cisco employs multiple technologies, procedures, and teams to ensure the secure operation of the Cisco Webex Meetings platform, including leveraging monitoring systems and diagnostic procedures to manage incident resolution during business-impacting events. Staff operators provide 24-hour coverage to detect incidents and to manage the impact and resolution.

Cisco has implemented key operational metrics and alarms across the production network using a variety of automated monitoring systems to detect outages, service latency, security incidents, and other unusual or unauthorized activities and conditions. Alarms are configured to notify operational and management personnel when warning thresholds indicating potential service latency, server unavailability, or other factors affecting availability and functionality are breeched. Personnel are on-call at all times to ensure that alarms are responded to in a timely manner.

Incidents and threshold warnings are logged in the incident tracking system. They are assigned a priority level and ownership and tracked through to appropriate resolution.

The Cisco Webex Meetings network utilizes IDS to protect against malicious code. IDS sensors are placed at a strategic point or points within the network to monitor traffic within the boundary and matches the traffic based on a library of known attacks. Once an attack is identified, or abnormal behavior is sensed, an alert is sent to the CSIRT team for corrective action in partnership with the product security team.

The Cisco network IDS is automatically updated whenever new releases are available in accordance with organizational configuration management policy and procedures.

Cisco network IDS is configured to automatically scan traffic. It also raises an alert in the event that malware is identified. Alerts are sent to CSIRT for investigation and ultimate remediation by the product team.

Cisco Webex Meetings incident management engages and coordinates with PSIRT and CSIRT (described elsewhere in this report) to investigate and report on security incidents.

Incident Response

CTG has established an incident response procedure defining actions when an event has been evaluated and is considered an incident. The Cisco Webex has developed and maintained an Incident Response Management procedure that includes which employees, contractors, and third-parties to contact in case of an incident and information security requirements needed for incident responses. The recommended process include:

- **Preparation** – actions to take in the event an incident occurs
- **Prevention** – Implementing practices to security networks, systems, and applications
- **Incident Detection and Analysis** – develop comprehensive procedures with step-by-step instructions for handling incidents
- **Incident Notification** – notifying appropriate individuals who need to be involved
- **Incident Containment, Eradication, and Recovery** – steps to take once an event is determined to be an incident
- **Post Incident Activity and Evidence Collection** – actions to meet regulator or contractual requirements; to identify and take corrective actions; to retain and provide evidence as needed
- **Incident Response Process Improvement** – identify opportunities to improve security measures, the incident handling process itself, reflect on new threats, and improved technology
- **Incident Response Metrics** – identify, capture, and measure metrics to gauge the effectiveness of the incident response capability

Event Logging

Cisco has established a *Security Logging Standard* that defines the requirements for logging data at Cisco. This policy establishes requirements for event types, time synchronization, content and other key information. Logs are centralized for aggregation, correlation, continuity, and retention.

This policy and standard includes requirements for:

- Security event logging and log content
- Security event alerting, analysis and reporting (monitoring)
- Log continuity management
- Integrity and protection of log information
- Audit record retention

End of Document