# Service Organization Control 3 (SOC 3®) Report

Enplug Inc.’s report on its DisplayOS Software relevant to Security for the period February 1, 2020 to January 31, 2021

ENPLUG

## Table of Contents

# Section I

# Enplug Inc.’s Management Assertion

ENPLUG

## Enplug Inc.'s Management Assertion

We are responsible for designing, implementing, operating and maintaining effective controls within Enplug Inc.'s ("Enplug") DisplayOS Software ("system") throughout the period February 1, 2020 to January 31, 2021, to provide reasonable assurance that Enplug's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in attachment A 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 February 1, 2020 to January 31, 2021, to provide reasonable assurance that Enplug's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Enplug's 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 attachment B.

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 February 1, 2020 to January 31, 2021, to provide reasonable assurance that Enplug's service commitments and system requirements were achieved based on the applicable trust services criteria.

Navdeep Reddy
Navdeep Reddy (Mar 13, 2021 15:46 PST)

Navdeep Reddy
Chief Information Officer
March 13, 2021

ENPLUG

# Section II

# Independent Service Auditor’s Report

MHM
Professional Corporation
Chartered Professional Accountant

## Independent Service Auditor's Report

To the Management of Enplug Inc.:

***Scope***

We have examined Enplug Inc.'s ("Enplug") accompanying assertion titled "Enplug Inc.'s Management Assertion" ("assertion") that the controls within the Enplug DisplayOS Software ("system") were effective throughout the period February 1, 2020 to January 31, 2021, to provide reasonable assurance that Enplug's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

***Service organization's responsibilities***

Enplug is responsible for its service commitments and system requirements and for designing, implementing and operating controls within the system to provide reasonable assurance that Enplug's service commitments and system requirements were achieved. In Section I, Enplug has provided the accompanying assertion titled "Management of Enplug's Assertion" ("assertion"), about the effectiveness of controls within the system. When preparing its assertion, Enplug is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

***Service auditors' 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 the Canadian Standard on Assurance Engagements 3000, Attestation Engagements Other Than Audits or Reviews of Historical Financial Information, set out in the *CPA Canada Handbook – Assurance* and with attestation standards established by the American Institute of Certified Public Accountants (AICPA). These 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 the description is not presented in accordance with the description criteria and that controls were not suitably designed

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Enplug's service commitments and system requirements based on the applicable trust criteria.
- 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 achieve the service organization's service commitments and system requirements based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design 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 the Enplug DisplayOS Software were effective throughout the period February 1, 2020 to January 31, 2021, to provide reasonable assurance that Enplug's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

***Restricted use***

Certain complementary subservice controls that are suitably designed and operating effectively are necessary, along with controls at Enplug, to achieve Enplug's service commitments and system requirements based on the applicable trust services criteria. Users of this report should have sufficient knowledge and understanding of complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements. Enplug uses Amazon Web Services (AWS) to provide cloud infrastructure services. Users of this report should obtain the relevant AWS SOC2 or SOC3 report.

*MHM Professional Corporation*

Chartered Professional Accountant
Calgary, Alberta
March 13, 2021

ENPLUG

# Attachment A

# Enplug Inc.’s Description of the Boundaries of its DisplayOS Software

ENPLUG

## Enplug Inc.'s Description of the Boundaries of its DisplayOS Software

*Types of Services Provided*

Enplug Inc. ("Enplug" or "the Company") is a provider of digital signage software, connecting business and institutions with their customers and employees. The Company runs screens around the world that show content from a variety of sources chosen by users. Enplug is headquartered in Culver City, CA, with partners in international locations such as Japan, Australia, and Europe.

Enplug's DisplayOS Software provides institutions and customers with an end-to-end solution that serves all stakeholders, domestic and cross-border. The digital signage software enables users to manage a network of displays that show content including webpages, graphics, videos, and social media.

*The Boundaries of the System Used to Provide the Services*

The boundaries of the system are the specific aspects of Enplug's infrastructure, software, people, procedures and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures and data that indirectly supports the services provided to customers are not included within the boundaries of the system.

The components that directly support the services provided to customers are as described in the sections below.

*Infrastructure*

The Company utilizes Amazon Web Services (AWS) to provide the resources to host the Enplug DisplayOS Software. Enplug leverages the experience and resources of AWS to enable Enplug to quickly and securely scale as necessary to meet current and future demand. However, Enplug is responsible for designing and configuring the Enplug DisplayOS Software architecture within AWS to ensure that security and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

| **INFRASTRUCTURE** | | | |
|---|---|---|---|
| **Production Tool** | **Business Function** | **Operating System** | **Hosted Location** |
| AWS Elastic Compute Cloud (EC2) | Hosting the services | Linux, Docker | AWS |
| MongoDB databases | Customer and analytics | Linux | AWS |

| | | | |
|---|---|---|---|
| | data storage | | |

*Software*

Software consists of the application programs and information technology (IT) system software that supports application programs (operating systems, middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the Enplug DisplayOS Software include:

| **SOFTWARE** | |
|---|---|
| **Production Application** | **Business Function** |
| Pingdom, InfluxDB | Application Monitoring |
| MongoDB | Logging System |
| Windows Server Updates | Patch Management |
| Trend Micro Deep Security | Anti-virus, intrusion detection |
| Zendesk, Jira | Helpdesk and ticketing system |
| AWS ECS, TeamCity and YouTrack | Configuration Management |

*People*

Enplug develops, manages, and secures the Enplug DisplayOS Software via separate departments. The responsibilities of these departments are defined as follows:

- Executive Management - Responsible for overseeing Company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- Engineering - Responsible for the development, testing, deployment, and maintenance of new code for the Enplug DisplayOS Software.
- Security Control Team - Responsible for access controls and security of the production environment. Includes the Chief Information Officer (CIO) and the Chief Software Architect.
- Human Resources - Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks and facilitating the employee termination process. Includes the Chief Executive Officer (CEO)

*Procedures*

Procedures include the automated and manual procedures involved in the operation of the Enplug DisplayOS Software. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, and human resources (HR). These procedures

are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than once annually.

- Logical and Physical Access - How the Company restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
- System Operations - How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
- Change Management - How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
- Risk Mitigation - How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

*Data*

Data refers to transaction streams, files, data stores, tables, and output used or processed by Enplug. The customer or end-user defines and controls the data they load and store in the Enplug DisplayOS Software production network via the platform. This data is loaded into the environment and accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest.

The following are the key data elements stored within Enplug databases:

- Usage Information
- Account and User Information
- Log Information

ENPLUG

# Attachment B

# Principal Service Commitments and System Requirements

## Principal Service Commitments and System Requirements

Enplug designs its processes and procedures related to its DisplayOS Software to meet its objectives. Those objectives are based on the service commitments that Enplug makes to user entities, the laws and regulations that govern SaaS providers, and the financial, operational, and compliance requirements that Enplug has established for the services.

Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the DisplayOS Software that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect customer data at rest and in transit.