PrinterLogic

Security Profile | FAQ

Last updated: March 13, 2020

CONFIDENTIAL

Introduction: This Security Profile comprises the most frequently asked security questions received and answered by PrinterLogic.
*For purposes of this document, the word "client" means PrinterLogic's customer.

Application: PrinterLogic SaaS Solution

Company Profile

Parent Company Name:	PrinterLogic, Inc.
Company/Business Name:	PrinterLogic, Inc.
Company Contact Information:	912 West 1600 South, Suite C201 St. George, UT 84770 Tel. Main: 435.652.1288
Length of Time in Business:	Since 2001
Type of Legal Entity and State of Incorporation:	Corporation, Delaware
Public or Privately Held Company:	Privately Held
Website:	printerlogic.com
PrinterLogic Security Team:	security@printerlogic.com

PrinterLogic Security Team Contact Information

Justin Scott - Director of Technology Operations
justin.scott@printerlogic.com

Martin Wright - General Counsel
martin.wright@printerlogic.com

Kenneth Adamson - Director of Engineering
kenneth.adamson@printerlogic.com

Corey Ercanbrack - Chief Technology Officer
corey.ercanbrack@printerlogic.com

Data Privacy

Q **Is there a designated organizational function responsible for data privacy or data protection?**

A Yes, PrinterLogic's Security Team is responsible for data privacy and data protection.

Q **Is there access to, processing of, or storage of any client data that includes personally identifiable information?**

A Yes. We store print job metadata including: job title, user, page count, and destination printer. For authorization we store usernames, names, and email addresses. In the event a client is not using an identity provider, we store authentication user information including passwords. We do not store any document content.

Data Privacy (continued) CONFIDENTIAL

Q Is there client data collected, transmitted, processed, or stored that can be classified as Protected Healthcare Information (PHI), special category data under GDPR (genetic data, biometric data, health data, etc.), financial/transactional information (PCI), or any other sensitive data?

A No. However, the title of a print job may include sensitive data. The storing of the print job title can be disabled.

Q Does PrinterLogic collect, access, process, or transmit any of client's customer's data?

A No.

Q Do subcontractors (e.g., backup vendors, service providers, software maintenance vendors, data recovery vendors, etc.) or other third parties have access to client systems or data?

A No.

Q Does PrinterLogic have a privacy policy?

A Yes. It is reviewed bi-annually.

Information Security: This section applies to the PrinterLogic company and its practices.

Q Is there a designated organizational function that reviews policies and procedures to assess risk, ensure information security, and assess compliance with applicable legal, regulatory, and industry requirements?

A Our security team owns all security policies and procedures and these are reviewed regularly.

Q Is there a set of information security policies that have been approved by senior management, published, and communicated to employees?

A Yes. These are reviewed annually by executive stakeholders.

Q Does the company maintain any specific information security compliance certifications (PCI, ISO, SOC, SSAE)?

A FIPS Certified, Common Criteria Compliant, pursuing SOC II or ISO 27001 certification in 2020.

Q Does the company manage its information security practices to an industry recognized security framework, such as ISO, SOC, or NIST?

A We follow the OWASP SAMM framework for governance, design, implementation, verification, and operations.

Q Do all PrinterLogic personnel undergo background checks in compliance with local laws prior to employment?

A Yes.

Q Do you require employees to sign a confidentiality agreement prior to employment? Does the agreement address client scoped data?

A Yes.

Q Are procedures in place to ensure proper IT asset access is managed following role change or termination of an employee?

A Yes.

Product Development Security: This section applies to the Software as hosted in AWS.

Q Are security requirements formally defined and tested for all development projects?

A Yes

Q Is there a documented patch management process?

A Yes. AWS controls patching of host systems. Virtual Machines in AWS are created from verified and immutable images. Base images are patched with latest security patches regularly and verified in testing environments. Container technology is utilized and upon upgrade, the entire image/container is refreshed from verified source.

Q Have penetration tests been conducted on client facing products or services?

A Yes. PL contracts with a security firm to conduct third-party penetration testing.

Q Are technologies and processes in place to backup and restore client data?

A Yes.

Q Do you encrypt client data in transit and at rest?

A Yes.

Access Control: Client Data within AWS

Q Are employees able to access client scoped data?

A There are a select number of employees who are members of the Operations team and that have access to client scoped data. Members of the Support team also may have access during certain troubleshooting support calls.

Q Are preventive, detective, and corrective controls in place to prevent unauthorized access to client scoped data?

A Yes.

Q Is multi-factor authentication required to access the production environment containing client scoped data?

A Yes.

Asset Management

Q Does the company maintain a formal inventory of its information technology assets?

A Yes.

Q Are processes in place to ensure all IT assets remain updated with anti-virus security?

A Yes.

Q Are procedures in place to ensure proper IT asset access is managed/removed after a role change or employee termination?

A Yes. All access to IT assets, systems, networks, and production environments (if applicable) is terminated immediately upon an employee termination or role change.

Data Management and Storage

CONFIDENTIAL

Q Does your company own and/or maintain the physical data center where the client data will reside?

A No. PrinterLogic SaaS is built and resides in Amazon Web Services (AWS).

Q Summary of physical security applicable to the data center.

A Details of physical security implementations for AWS are found both at **www.infrastructure.aws** and https://aws.amazon.com/compliance/data-center/controls/

Q If the environment is multi-tenant, how is a client's data segregated from the other customer data?

A The environment is multi-tenant but the customer database is separated from other customer databases.

Q In the event that services are terminated, can all of client's data be returned to client?

A Yes.

Q Will any of PrinterLogic's vendors have access to client data?

A No. No third parties have access to client scoped data.

Business Continuity/Disaster Recovery

Q Do you have a Disaster Recovery plan?

A Yes.

Q Does PrinterLogic test its Disaster Recovery Plan (DRP)?

A Yes. Twice a year.

Risk and Security Incident Management

Q Is there a formalized risk governance and continuous risk assessment program that identifies, quantifies, and prioritizes risks?

A Yes. This is governed by the PrinterLogic Security Team.

Q Does PrinterLogic maintain a security incident management program?

A Yes.

Q Does PrinterLogic carry appropriate levels of general liability Insurance and does that insurance include Tech E&O and Cybersecurity?

A Yes. A Certificate of Insurance (COI) can be produced upon request.