

# PROOFPOINT INSIDER THREAT MANAGEMENT SAAS

These detailed Appendices form part of the Clauses and are deemed have to been incorporated into the Clauses when the parties signed page 1 of the Proofpoint Data Processing Agreement.

## APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

### 1. **Data exporter**

The data exporter is **data exporter's affiliated European companies**

The data importer's Insider Threat Management (ITM) SaaS services ("Services") tracks data exporter's users endpoint activities, including any Personal Data processed or stored within those endpoints . The data exporter hereby provides standing instructions for data importer to implement and use the Services to track endpoint activity in order to protect the data exporter from malicious and potentially illegal activities by its users.

### 2. **Data importer**

The data importer is **Proofpoint, Inc.**

Data importer provides its on-demand ITM services from its US-based datacenters hosted by Amazon Web Services.

### 3. **Data subjects**

Data subjects are data importer's End users:

- a) ITM SaaS Administrators or analysts, using the web portal.
- b) Endpoint users, using data exporter's endpoints on which the ITM SaaS agent has been installed.

### 4. **Categories of data**

Personal Data used or stored by ITM includes: email address, device identifier such as IP address, user information such as name and user ID, website information such as URL and page name, Application information such as application name, executable name, and window title. Additionally, ITM has the capability to capture screen content, which is configured and controlled by the data controller. Screen capture could include any additional personal data displayed on the user's screen.

### 5. **Processing operations**

#### ITM Processes

- ITM deploys an endpoint agent onto designated laptop, desktop and server devices owned or controlled by data controller. The agents collect telemetry data about the activities of the device users, the data subjects. If enabled by data controller the agents can also capture screenshots of the users' device activities. Controller solely determines whether to enable the screen capture capabilities, and the data retention period of such content. The telemetry and screen capture data is stored on Proofpoint's multi-tenant ITM SaaS storage, which is hosted in AWS in the US.

6. **Correction, deletion and blockings of data**

Data importer may only correct, delete or block the data processed on behalf of the data exporter when instructed to do so by the data exporter, however the parties recognize and agree that only the data exporter can correct, delete or block the user's access to the ITM Service.

7. **Data exporter's right to issue instructions**

The Services Agreement between the data exporter and the data importer are the instructions for the data processing. Data exporter may provide any additional instructions in writing to data importer via amendment or via the data importer's technical support portal.

Data importer shall inform the data exporter promptly upon reasonable belief that there has been an infringement of an applicable statutory data protection provision. Data importer may postpone the execution of the relevant data exporter instruction until it is confirmed or changed by the data importer's representative.

**APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES**

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

**Summary of Proofpoint Internal Processes**

**A. Summary**

This document summarizes the processes and procedures that Data Importer implements in conjunction with the provision of the Services.

**B. Control Group**

***Identification and authentication of the user***

There are two classes of users that interact with the Services:

Data Exporter users: Data Exporter administrative users potentially may access personal data when logging into the administrator portal through a web-browser based user interface.

Data Importer users: Centralized authentication and logging is used to ensure that only approved Data Importer personnel have access to the infrastructure supporting the Service. All members of the team responsible for the Service receive specific training in the administration of the Services, in addition to annual Security Awareness training.

***Data Importer Controls***

Management has established and approved an information security policy.
A framework of security standards has been developed, which supports the objectives of the security policy.
Procedures exist for and to ensure adherence to, authenticating and authorizing users to systems.
Procedures exist for and to ensure adherence to policies for requesting, establishing, issuing, suspending, deleting, and closing user accounts and associated access privileges, e.g. system access is granted based upon position, job function, and manager approval.
A process is in place to monitor failed login attempts. Identified security violations are resolved.
Access to the Data Importer production environment by employees is based on business need. A two-factor authenticated VPN is utilized.
Controls are in place to restrict implementation of changes to production only to authorized individuals.

***Type of access***

The various types of Data Exporter user access are documented in the Administrator Guide and are controlled by Data Exporter administrators.

**C. Collection of data**

User initiates authentication to the ITM SaaS service using the data exporter's identity provider (IdP). Connection is established using an encrypted HTTPS connection.

**Data Importer Controls**

Encrypted network connections are used to protect Data Exporter data in transit between endpoints and the hosted components of the Service. Each Data Exporter can only access their own data.

**D. Execution of backup copies**

**Data Importer Controls (Services only)**

Procedures for backup and retention of data and programs have been documented and implemented.
Data and programs are backed up regularly and replicated within multiple AWS availability zones.

**E. Computers and access terminals**

Computers used by Data Importer employees to access the Data Importer infrastructure require multi-factor authentication to access the AWS instance(s) containing Data Exporter data. All computers are required to run up to date anti-virus software and policies and procedures exist to restrict software that may be installed on these machines. All Data Importer employees are required to authenticate to a centralized authentication system in order to access the Data Importer corporate and production networks.

**Data Importer Controls**

New employees are required to sign a non-disclosure agreement relating to proprietary software and confidentiality of information relating to customers.
New employees also receive a summary of Data Importer's information security program, which they are required to acknowledge receipt of.
Access to the Data Importer production environment by Data Importer employees is based on business need. Two-factor authentication is utilized.

**F. Access logs**

In relation to the Services, access logs take at least two different forms:

- 1 - All access attempts to Data Importer computer systems are centrally logged and unusual activity is automatically reported to Data Importer Global Information Security group.
- 2 – All access attempts by Data Exporter to hosted Services are logged and are available to Data Exporter.

**Data Importer Controls**

Procedures exist for and to ensure adherence to, authenticating and authorizing users to systems.
A control process exists and is followed to periodically review and confirm access privileges remain authorized and appropriate.
A process is in place to monitor failed login attempts. Identified security violations are investigated and resolved.
Application event data are retained to provide chronological information and logs to enable the review, examination, reconstruction of data processing and application events.

**G. Telecommunication systems**

Data Importer leverages AWS to provide redundant network connections for the hosted portions of the ITM Services.

**H. Instruction of personnel**

All Data Importer personnel are required to complete an annual Security and Awareness training program offered online. In addition, members of the Data Importer Global Information Security group receive on-going training specific to their roles. This training may be provided internally or through third-party organizations.

**Data Importer Controls**

Data Importer has an organization plan, which separates incompatible roles and duties of relevant personnel.
Separate management roles and responsibilities have been designed to segregate the roles of computer operations, system development and maintenance, and general Data Importer corporate functions.
Personnel roles and responsibilities are clearly defined.

**I. Use of computers**

Access to Data Importer production networks is restricted to systems running Data Importer-approved and managed anti-virus software. As well, all Data Importer computer systems used to access the Data Importer production network are connected to a centralized authentication system. All Data Importer employees are made aware of Data Importer acceptable use policies for Data Importer computers and internet access. Data Importer employees must acknowledge these policies and sign a document stating they agree to abide by them.

**Data Importer Controls**

New employees are required to sign a non-disclosure agreement relating to proprietary software and confidentiality of information relating to customers.
New employees also receive a copy of Data Importer's Employee Handbook.

**J. Printing of data**

There are no printing services available in the Data Importer's AWS instance – no data is printed.

**Data Importer Controls**

New employees are required to sign a non-disclosure agreement relating to proprietary software and confidentiality of information relating to customers.
New employees also receive a copy of Data Importer's Employee Handbook.

**K. Physical Access Control**

**Data Importer Controls**

Data Importer has no physical access to the AWS instance used to host the ITM Service.

**L. Physical Security Measures for AWS Hosting Environment**

Country	Address	Personal Data processed	Approved Services for this location
USA	East Coast	See Appendix 1, Section 4, Categories of Data	ITM services are hosted in Data Importer's instance of Amazon Web Services. Physical access is controlled by AWS.

**Data Importer Controls**

The hosting facilities utilized by AWS are aligned with Tier-3 data center standards and include the following:

1. 24x7 on-site security
2. 24x7 on-site and remote facilities monitoring
3. Single point of access
4. Dual-factor authentication required for access
5. Anti-piggybacking devices in place
6. Cameras at all entrances and exits.
7. Fences, gates and barriers are in place.
8. Locked shipping docks with no direct access to facility floor.
9. VESDA-type smoke detection
10. Dual-action dry-pipe fire suppression system
11. Redundant power, including battery UPS and on-site generators
12. Redundant environmental controls in N+1 configuration

**M. Access control to IT systems**

**Data Importer Controls**

Data Importer controls access to systems providing Services in the following ways:

1. All Data Importer employees and contractors are provided with unique userIDs. Account sharing is not permitted.
2. Password requirements are defined and enforced by a password synchronization tool. Requirements include:
  - a. Minimum of 12 characters
  - b. May not appear on public and Data Importer-maintained lists of breached passwords
  - c. History of 23
  - d. Required to change every 180 days
  - e. Account locked out after five (5) failed login attempts
3. Logical access is granted based on role.
  - a. Only members of the Operations group are granted privileged access to the Data Importer production environment.

- b. All members of this group are required to use 2FA when accessing the Data Importer production environment.
4. Security audit logs are directed to a log aggregation and alerting tool. Alerts are configured to be sent to the Data Importer Global Information Security group.

**N. Access control to data**

**Data Importer Controls**

Data Exporter data is not permitted to reside in the Data Importer corporate environment. Access to Data Exporter data are controlled in the following ways:

1. Access is granted based on role at Data Importer, with a business need.
2. Only the Data Importer Operations group is permitted to have privileged access to the Data Importer production environment.
3. Privileged access lists are reviewed monthly.

- O. Audit logging is in place on systems in the Data Importer Production Environment.**

**P. Implement least privilege access control**

**Data Importer Controls**

Access to the Data Importer Production Environment is granted based on role and business need. Only members of the Data Importer Operations group are granted privileged access to the Production Environment. Privileged access is reviewed monthly to ensure it remains appropriate.

**Q. Security while transferring and processing**

**Data Importer Controls**

Data Importer does not permit Data Exporter data to reside in the Data Importer Corporate Environment, where Data Importer employees and contractors reside. The Data Importer Production Environment is logically and physically segregated from the Data Importer Corporate Environment:

1. Access to the Data Importer Production Environment is via a two-factor authentication and is only provided to Data Importer employees and contractors whose role requires access.
2. Network ACLs and AWS Security Groups are in place and configured to only permit traffic on ports necessary for the functioning of the Service with all others denied by default.
3. All intra-Service communications are encrypted using TLS.
4. All Administrator and User access to the Services hosted web interfaces is encrypted using TLS.

**System Access Controls**

1. Identity provider service is used to manage access.
2. Privileged access is only granted to members of the Data Importer Operations group whose roles require access.

**Endpoint Security**

1. Network ACLs and AWS Security Groups are in place and configured to only permit traffic on ports necessary for the functioning of the Service with all others denied by default. All endpoints in use by Data Importer employees must have a centrally managed anti-virus solution installed

#### ***Server Security***

1. Operating systems are patched.
2. Unnecessary services are disabled.
3. Default passwords are changed.

#### **R. *Security while transmitting data over public networks***

##### ***Data Importer Controls***

1. All intra- Services communications are encrypted using TLS.
2. All Administrative and User access by Data Exporter to the Services is encrypted using TLS.

#### **S. *Implementation and Operations phase controls***

##### ***Data Importer Controls***

The functionality provided by the Services is performed automatically and does not require human intervention, except in order to troubleshoot issues with the Services. The Services are designed to function as described in the Services Agreement. Monitoring is in place to ensure that the Services are functioning as described in the Services Agreement including alignment with applicable SOC 2 trust services criteria.

#### **T. *Monitoring and Testing phase controls***

##### ***Data Importer Controls***

The functionality provided by Services is performed automatically and does not require human intervention, except in order to troubleshoot issues with the Services.

#### **U. *Traceability of any access, change and deletion***

##### ***Data Importer Controls***

Access to systems hosting Data Exporter data are controlled in the following ways:

1. Access is based on role at Data Importer.
2. Only the Data Importer Operations group is permitted to have privileged access to the Data Importer Production Environment.
3. Privileged access lists are reviewed monthly.
4. Audit logging is in place for systems in the Data Importer Production Environment.



The Service controls access in the following way:

1. Administrative access to the Administrator Web Interface by Data Exporter administrators is granted by Data Importer at the request of Data Exporter or by the Data Exporter itself.
2. End-User access to the End-User Web Interface by Data Exporter end-users is granted by Data Exporter through the use of IDP.
3. The Services generate Application Logs that include Administrator and End-User access and include the following:
  - a. Successful/Failed login attempts
  - b. Date
  - c. Time
  - d. Source IP
  - e. userID

## **V. *Ensuring Compliant Data Processing***

### ***Data Importer Controls***

Data Importer personnel do not manually process Data Exporter data. All Data Exporter data is automatically processed by the Services, as described in the Services documentation.

## **W. *Ensuring Availability***

### ***Data Importer Controls***

The Services are architected to ensure Availability in-line. This is accomplished in the following way:

1. The Services are configured to replicate Data Exporter data across multiple AWS availability zones.
2. The Service is hosted within AWS. AWS physical environments are aligned with Tier-3 data center standards.
3. Data Exporter data is backed up daily for Disaster Recovery purposes.
4. A documented Disaster Recovery Plan is in place.
5. A documented Business Continuity Action Plan is documented and tested annually.
6. A distributed monitoring infrastructure monitors for Availability.
7. Network ACLs and AWS Security Groups are configured to permit ports necessary for the Service and deny all others by default.
8. All Data Importer owned Windows and Mac laptops, workstations and servers in the Data Importer corporate environment run a centrally-controlled anti-virus service.

## **X. *Data Separation***

### ***Data Importer Controls***

The Services maintain logical segregation of Data Exporter data.