

# PROOFPOINT CLOUD ACCOUNT DEFENSE (CAD) AND CLOUD APP SECURITY BROKER (CASB)

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 Cloud Account Defense and Cloud App Security Broker services ("Services") protect data exporter and its Affiliates from advanced threats, accidental sharing and compliance risks in the cloud accounts such as Microsoft 365 OneDrive and Google Drive. PCASB's powerful analytics help you grant the right levels of access to users and third-party apps based on the overall risk factor.

### 2. **Data importer**

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

Data importer provides its on-demand Services from Amazon Web Services' hosted cloud platform in Amazon's US-based datacenters.

### 3. **Data subjects**

To the extent there is Personal Data processed by the Services the following categories of data subjects may apply: data exporter's end-users including employees and contractors.

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

To the extent there is Personal Data processed by the Services the following categories of data may apply: end-user metadata (e-mail addresses, names, position), file metadata and end-user activity.

### 5. **Processing operations**

The CAD and CASB services securely store and utilise end-user metadata (e-mail addresses, names, position), file metadata and end-user activity to block unauthorized access of Data exporter's online storage accounts, and based on policies the Data exporter selects, to prevent the authorized transfer of data and files outside of Data exporter's cloud accounts.

### 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.

### 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.

Data exporter shall pay for data importer costs and expenses for any audit under Model Clause Section 5 Obligations of the Data Importer, provided however, in the event that data exporter pays data importer annual Services subscription fees of more than USD 250,000, then data exporter and data importer shall each pay for its own costs and expenses for any audit under Model Clause Section 5 Obligations of the data.

## **APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES**

Description of the technical and organisational 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 Cloud Account Defense and Cloud App Security Broker Services.

#### **B. Control Group**

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

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

Data Exporter end-users: Data Exporter administrative users and email recipients potentially may access personal data by viewing the EFD reporting interface.

Data Importer users: Centralized authentication and logging is used to ensure that only approved Data Importer personnel have access to the Data Importer data centers and the Services infrastructure, including the back-end services that analyze collect email metadata and attachments. All members of the Operations team 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 authorized by the Director of operations and the relevant department head, and 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 end user access are documented in the Administrator Guide and are controlled by Data Exporter administrators through the Services dashboard or user interface

**C. Collection of data**

End-user metadata (e-mail addresses, names, position), file metadata and end-user activity configured by the Data Exporter in the Services are monitored for unauthorized use and fraudulent activity based on rules configured by Data Exporter.

**Data Importer Controls**

Data Exporter data is not stored in the Service; encrypted network tunnels are used to protect Data Exporter data in transit whenever possible, and Data Exporter Data at rest is protected whenever possible with unique encryption keys. Data Exporter's access is limited to only their own data.

**D. System Redundancy**

Data Exporter's data is hosted in redundant AWS implementations to protect against data loss.

**Data Importer Controls**

Redundancy is configured through Amazon Web Services.

**E. Computers and access terminals**

Computers used by Data Importer employees to access the Data Importer infrastructure are required to use a secure VPN tunnel to access the Data Importer infrastructure. 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 copy of Data Importer's security code of conduct, which they are required to acknowledge receipt of.
Access to the Data Importer production environment by employees is authorized by the Director of operations and the relevant department head, and is based on business need. A two-factor authenticated VPN is utilized.

**F. Access logs**

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

All access attempts to Data Importer computer systems are centrally logged and unusual activity is automatically reported to Data Importer Security Operations group. In addition, Data Importer enforces account lockout policies, password complexity requirements, and password age requirements. Logs of customer access to the Email Fraud Defense services are generated and retained according to Proofpoint standard policies and procedures.

**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 systems and data processing and application events.

**G. Telecommunication systems**

All Data Importer production data centers have redundant internet feeds from diverse bandwidth providers..

**H. Instruction of personnel**

All Data Importer personnel are required to complete an annual Security and Awareness training program offered online through a third-party training organization. In addition, members of the Data Importer Security Operations team receive on-going training specific to their roles. This training may be provided by vendors or other 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 are managed by a centralized authentication system. All Data Importer employees are made aware of Data Importer acceptable use policies for Data Importer computers, internet access and email communications. 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 review and acknowledge Data Importer’s Security Code of Conduct.

**J. Printing of data**

Data Exporter data is processed in memory and is not available for printing. In addition, there are no printers available within the Data Importer production data centers and all print services are disabled by default on all production servers.

**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 review and acknowledge Data Importer’s Security Code of Conduct.

**K. Physical Access Control**

**Data Importer Controls**

Data Importer maintains controls over physical access to the Data Importer Production Environment according to the AWS Physical Access Control standards.

**L. Physical Security Measures for Data Centers**

As set forth by AWS Physical Access Control Standards.

**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. Complexity rules (3 of 4 – upper, lower, numbers, special characters)
  - c. History of 23
  - d. Required to change every 60 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.
4. Audit logging is in place on the VPN to the Data Importer Production Environment.
5. Audit logs are monitored in near real-time by a log aggregation and alerting tool. Alerts are configured to be sent to the Data Importer Security Operations 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 systems hosting the Service are controlled in the following ways:

1. Access is based on role at Data Importer.
2. Only authorized personnel at the Data Importer are permitted to have privileged access to the Data Importer EFD Production Environment.

**O.** Audit logging is in place on the VPN and 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. Only authorized members of the Data Importer team are granted privileged access to the Production Environment..

**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 authenticated VPN and is only provided to Data Importer employees and contractors whose role requires access.
2. Industry-standard firewalls 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. .
4. All intra-Service communications are encrypted using TLS.
5. All Administrator access to the Services hosted web interfaces is encrypted using TLS.

**System Access Controls**

1. LDAP is used to manage access.
2. Privileged access is only granted to authorized Data Importer personnel.

**Endpoint Security**

1. Industry-standard firewalls are in place and configured to only permit traffic on ports necessary for the functioning of the Service with all others denied by default.
2. .

**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. .
2. All intra- Services communications are encrypted using TLS.
3. All Administrative 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.

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

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

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

1. Access is based on role at Data Importer.
2. Only authorized personnel are permitted to have privileged access to the Data Importer Production Environment.
3. Audit logging is in place on the VPN and on 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.
2. The Services generate Application Logs that include Administrator access and include the following:
  - a. Successful/Failed login attempts
  - b. Date
  - c. Time
  - d. Changes to configuration
  - e. Changes to data

#### **U. *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.

#### **V. *Ensuring Availability***

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

The Services rely on and leverage Amazon Web Services' security standards to ensure Availability



**W. Data Separation**

***Data Importer Controls***

The Services maintain segregation of Data Exporter data. This is accomplished in the following way:

1. Logical segregation is maintained by the service using unique Client IDs for each client that are used to tag client data within the service.

Data Exporter data is not permitted in the Data Importer Development or QA environments without being specifically requested in writing by the Data Exporter as part of a troubleshooting exercise.

**Appendix 3  
Subprocessors**

<b><u>Subprocessor Name</u></b>	<b><u>Location</u></b>
Amazon Web Services (AWS)	USA