

# Attestation Template for Unauthorized Data Transfer & Deletion

## Description:

The following is an example template provided for general informational purposes only. Organizations may modify and distribute to employees in the event they find themselves implicated in an Insider Risk Data Incident. Consult with your General Counsel prior to utilizing this template.

## Unauthorized Data Transfer & Attestation

Data protection is a critical component of **[Company Name]**. In an evolving threat landscape, the effective protection of data helps safeguard an organization and establish a company's reputation as an entity employees and consumers alike can trust with their data.

In accordance with **[Company Name]** guidelines, during the onboarding process you signed an Employee Agreement with **[Company Name]** and agreed to abide by the Corporate Security Policy. Both your Employee Agreement and Corporate Security Policy require you to protect the confidentiality of data belonging to **[Company Name]**. You may only use **[Company Name]** data and resources as required to conduct your job duties and only on **[Company Name]** approved devices, systems, and trusted domains.

We observed a transfer of **[Company Name]** data in violation of your Employee Agreement and the Corporate Security Policy, as described in Exhibit A ("Unauthorized Transfer Documentation or Evidence").

## Due to the seriousness of this matter, we require that you agree and acknowledge that:

- You have permanently deleted all **[Company Name]** data involved in the transfer (including any copies, duplicates, subsets, extracts, derivatives and related materials) from all unauthorized devices and systems
- You have not transferred any other **[Company Name]** data to unauthorized devices or systems (if such a transfer was in fact performed, it has since been resolved).
- You have not provided access to **[Company Name]** data to an unauthorized third party (if such access was in fact granted, it has since been revoked).
- You have reviewed and acknowledged **[Company Name]** corporate security policy and understand your responsibilities with regards to **[Company Name]** data

***Any transfers of [Company Name] data, or attempts to transfer [Company Name] data, to an unauthorized device or system may result in disciplinary action, including termination.***

If you have any questions regarding this matter or whether a device or system is approved for [Company Name] data, please contact the security team (contact@securityteamemail) or legal team (contact@legalteamemail).

**Attest: Under penalty of perjury, I hereby attest to the best of my knowledge that the information herein is true and correct.**

**Name (Print)** \_\_\_\_\_

**Signature** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Exceptions: If you answered "NO" to any question or believe a question is not applicable, please contact the privacy / compliance officer. All "NO" or "N/A" answers must be reviewed by the privacy / compliance officer or designated representative.**

**Name (Print)** \_\_\_\_\_

**Signature** \_\_\_\_\_

**Date:** \_\_\_\_\_

## **Exhibit A** [Attachment documentation of unauthorized transfer]