Georgian American University, LLC

Employee Responsibilities and Obligations During Personal Data Protection Incidents

Contents

Introduction

This document defines the responsibilities and obligations of employees regarding the protection of personal data. It is essential for all employees to understand their duties to ensure compliance with data protection laws and to prevent incidents.

Purpose

The purpose of this document is to:

- Define the responsibilities of employees in protecting personal data.
- Establish the consequences of failing to ensure personal data protection.
- Describe procedures to follow in the event of a data breach.

Scope

This policy applies to company employees, contractors, and third-party service providers who have access to personal data processed by the company.

Employee Responsibilities

Employees are required to:

1. Comply with data protection laws and the company's policies regarding personal data protection.
2. Ensure the confidentiality, integrity, and availability of personal data.
3. Access, use, and share personal data only for legitimate business purposes.
4. Protect personal data from unauthorized access, disclosure, alteration, or destruction.
5. Immediately report any incidents or suspected incidents to the Data Protection Officer (DPO) or their direct manager (if applicable).

Data Protection Measures

Employees must:

1. Use strong passwords and change them regularly.
2. Lock or turn off computers and mobile devices when not in use.
3. Use encryption tools for special categories of data.
4. Avoid unauthorized sharing of personal data.
5. Follow the company's protocols for data transmission and storage.

Incident Response

In the event of a data breach or suspected breach, employees must:

1. Immediately report the breach to the DPO or their direct manager (if applicable).

2. Preserve any evidence related to the breach.
3. Cooperate fully in the investigation, resolution, and prevention of future breaches.
4. Avoid discussing the incident with unauthorized individuals.

Failure to comply with these responsibilities may result in disciplinary action, up to and including termination of employment.

Individual Employee Responsibility

Employees may be held accountable for:

1. Intentional or negligent violations of the personal data protection policy.
2. Failing to report an incident they are aware of.
3. Actions that cause financial or reputational harm to the company.

Disciplinary Action

Non-compliance with this policy may result in disciplinary measures, including:

- Verbal or written warnings.
- Formal reprimands.
- Termination of employment.
- Legal action, if necessary.

Training and Awareness

Employees will undergo training on data protection laws, company policies, and best practices for safeguarding personal data. This ensures they are equipped to handle data responsibly and comply with regulations.

Review and Updates

This document will be reviewed and updated regularly to ensure alignment with current laws and regulatory requirements.