**Company K Data Security Policies**

**1. Purpose**

The purpose of this policy is to safeguard Company K's data and ensure that all employees, contractors, and third-party collaborators understand and adhere to the necessary data protection measures. This policy outlines the standards for handling sensitive, confidential, and proprietary data to prevent unauthorized access, data breaches, and other security risks.

**2. Scope**

This policy applies to all employees, contractors, and third-party collaborators who handle Company K's data, including personal data, intellectual property, client information, financial records, and any other sensitive information. It covers data stored on company devices, networks, cloud systems, and external storage media.

### **3. Key Data Security Principles**

Company K's data security policies are based on the following principles:

* **Confidentiality**: Only authorized personnel should access sensitive information.
* **Integrity**: Ensure data accuracy and prevent unauthorized modifications.
* **Availability**: Ensure authorized users have access to data and systems when required.
* **Accountability**: Ensure that every employee is responsible for protecting the data they handle.

### **4. Data Classification**

Data at Company K is classified into three categories to ensure appropriate levels of security based on sensitivity:

#### **4.1 Public Data**

* Data that can be freely shared with the public (e.g., marketing materials, website content).
* **Protection Requirements**: Minimal security; no confidentiality measures required.

#### **4.2 Internal Use Only**

* Data that is accessible to Company K employees but should not be shared externally (e.g., internal reports, employee directories).
* **Protection Requirements**: Moderate security; access controls must be in place.

#### **4.3 Confidential Data**

* Sensitive data that is strictly limited to specific employees, departments, or teams (e.g., client data, financial records, trade secrets).
* **Protection Requirements**: High security; encryption, strong access controls, and additional safeguards required.

### **5. Data Handling Guidelines**

#### **5.1 Access Control**

* **Least Privilege**: Employees should only have access to the data necessary to perform their job functions.
* **Multi-Factor Authentication (MFA)**: Required for access to critical systems and sensitive data.
* **Role-Based Access**: Data access will be granted based on employee roles (e.g., HR, IT, Finance), ensuring employees can only view relevant data.
* **Periodic Audits**: Access levels will be regularly reviewed by the IT and Security teams to ensure that employees’ access remains appropriate for their current role.

#### **5.2 Data Transmission**

* **Encryption**: All sensitive data transmitted over networks (including email, cloud services, or file transfers) must be encrypted using industry-standard encryption protocols (e.g., SSL/TLS).
* **Secure Channels**: Employees must use secure channels (e.g., VPN, encrypted emails) when accessing or sharing sensitive data remotely.

#### **5.3 Data Storage**

* **Encryption at Rest**: Confidential data must be stored in encrypted form, whether on company devices, servers, or in the cloud.
* **Cloud Security**: Data stored in cloud services (e.g., Microsoft Azure, AWS, Google Cloud) must be protected by strong access controls and encryption.
* **Removable Media**: Storing sensitive data on external or removable media (e.g., USB drives) should be avoided. If necessary, these devices must be encrypted and securely stored.

### **6. Device and System Security**

#### **6.1 Device Security**

* **Passwords**: All company devices (e.g., laptops, smartphones, tablets) must be protected by strong, unique passwords that adhere to the **Password Management and Reset** policy.
* **Screen Lock**: Devices must be configured to automatically lock after a period of inactivity (e.g., 10 minutes).
* **Antivirus & Malware Protection**: Devices must have up-to-date antivirus and anti-malware software installed.
* **Mobile Device Management (MDM)**: Company-issued mobile devices will be managed through an MDM solution, allowing IT to enforce security policies and remotely wipe data if a device is lost or stolen.

#### **6.2 Network Security**

* **Virtual Private Network (VPN)**: Employees must use Company K’s VPN when accessing the internal network remotely or from public Wi-Fi networks.
* **Firewalls**: Company systems will be protected by firewalls to prevent unauthorized network access.
* **Wi-Fi Security**: Employees should use secure Wi-Fi networks (e.g., WPA2 encryption) and avoid connecting to public or unsecured Wi-Fi for work purposes.

### **7. Data Backup and Recovery**

* **Regular Backups**: Company K will perform regular backups of critical data to prevent data loss due to hardware failures, cyber-attacks, or other incidents.
* **Backup Encryption**: All backup data must be encrypted.
* **Disaster Recovery Plan**: Company K has a disaster recovery plan that includes procedures for restoring data from backups in the event of a data loss incident.

### **8. Data Breach Response**

In the event of a data breach, Company K will follow a formal incident response process to contain the breach, investigate the cause, and mitigate its impact.

#### **8.1 Incident Reporting**

* Employees must report any data security incidents, including suspected breaches or unauthorized access, to the IT Security team immediately.
* IT will initiate the **Incident Response Plan**, which includes investigation, documentation, and reporting to the relevant stakeholders.

#### **8.2 Data Breach Notification**

* In the event of a significant data breach involving sensitive information, affected employees, clients, and regulatory authorities will be notified within the required time frame (e.g., 72 hours for GDPR compliance).

### **9. Compliance and Legal Obligations**

Company K complies with all relevant data protection regulations, including but not limited to:

* **General Data Protection Regulation (GDPR)**: For the protection of personal data belonging to individuals within the European Union.
* **California Consumer Privacy Act (CCPA)**: For protecting the privacy of California residents.
* **Health Insurance Portability and Accountability Act (HIPAA)**: For protecting personal health information (if applicable).

Employees must follow these legal obligations and ensure all data is handled in compliance with local and international data protection laws.

### **10. Employee Responsibilities**

All Company K employees are responsible for safeguarding company data. This includes:

* **Adhering to Security Policies**: Employees must follow this data security policy and report any non-compliance or suspicious activity.
* **Protecting Sensitive Data**: Employees must handle sensitive data responsibly and avoid sharing it outside of authorized channels.
* **Training**: All employees will receive regular training on data security best practices and updates to Company K’s policies.

### **11. Consequences of Policy Violations**

Violations of Company K’s data security policies can lead to disciplinary actions, including termination of employment, legal action, and financial penalties for the employee or contractor involved.

Deliberate data breaches, such as sharing confidential data without authorization, will result in immediate termination and potential legal consequences.

### **12. Policy Updates**

This policy will be reviewed and updated annually or as required by changes in data security laws or Company K’s business needs. Employees will be notified of any significant changes and are expected to stay informed about current policies.

### **13. Contact Information**

For questions about the Data Security Policy or to report a security incident, please contact:

* **IT Security Team**: it-security@companyk.com
* **IT Support**: it-support@companyk.com