**Company K Access to Internal Tools/Systems**

**1. Purpose**

This document provides guidelines for requesting, granting, and managing access to Company K’s internal tools, systems, and resources. It ensures secure and efficient access while protecting sensitive company information.

**2. Scope**

These guidelines apply to all Company K employees, contractors, and third-party collaborators who need access to internal tools or systems, including but not limited to HR systems, project management tools, CRMs, communication platforms, and development environments.

### **3. Requesting Access**

#### **3.1 New Employees**

Upon joining Company K, new employees will be granted access to the systems and tools relevant to their role. The Human Resources (HR) department will coordinate with the IT department to ensure new employees receive access within their first week of employment.

##### **Steps for Access Setup:**

1. **HR Notification**: HR submits an access request to IT, specifying the tools required for the employee's position.
2. **IT Configuration**: IT will create user accounts for systems like:
   * Company K Email
   * Employee Portal (HR)
   * Project Management Tools (e.g., Jira, Asana)
   * Internal Communication Tools (e.g., Microsoft Teams, Slack)
   * Department-Specific Tools (e.g., CRM for Sales, Development Tools for IT)
3. **User Notification**: The employee will receive login credentials and setup instructions via email.

#### **3.2 Role-Specific or Additional Access**

Employees may need access to additional tools or systems beyond what is initially provided, based on project requirements or changes in their role.

##### **Steps to Request Additional Access:**

1. **Submit Access Request**: Employees or their managers must submit a request through the **IT Helpdesk Portal** or via email to IT at it-support@companyk.com.
2. **Manager Approval**: For high-level or restricted tools, the employee’s manager must approve the access request.
3. **IT Provisioning**: IT will review the request, configure the appropriate access, and notify the employee of the new system access.

#### **3.3 Contractors and Third-Party Collaborators**

External contractors or third-party collaborators may require temporary access to certain systems or tools. Access for these individuals is governed by strict guidelines to ensure the security of Company K’s data.

##### **Steps for Granting Temporary Access:**

1. **Sponsor Request**: The Company K sponsor (an internal employee responsible for the contractor) submits an access request to IT.
2. **Security Review**: IT performs a security assessment to determine the level of access required.
3. **Granting Access**: IT configures access with an expiration date. Access will automatically be revoked when the contract ends unless otherwise specified.

### **4. Access Management**

#### **4.1 Role-Based Access Control (RBAC)**

Company K uses Role-Based Access Control (RBAC) to manage access to tools and systems. Employees are grouped based on their roles (e.g., Marketing, IT, Sales), and access is granted according to the resources they need to perform their duties.

* **Examples**:
  + **HR Employees**: Access to payroll systems, employee records, and HR dashboards.
  + **Sales Employees**: Access to CRM, lead management tools, and sales analytics.
  + **IT Employees**: Access to development environments, databases, and system monitoring tools.

#### **4.2 Regular Access Audits**

To maintain security, IT will conduct regular access audits to ensure that only authorized personnel have access to critical systems and sensitive information.

* **Frequency**: Audits will be performed quarterly or during major organizational changes (e.g., team restructuring, mergers).
* **Audit Process**: Department heads will review current access rights and notify IT of any necessary changes or revocations.

#### **4.3 Revoking Access**

Access to Company K’s internal tools and systems will be revoked upon termination, resignation, or role change. Immediate termination cases (e.g., security violations, breaches of company policy) will result in urgent access revocation.

##### **Steps for Access Revocation:**

1. **HR Notification**: HR will notify IT of any terminations or resignations.
2. **IT Action**: IT will revoke all access to internal systems on the employee’s last working day, or sooner if required for security reasons.
3. **Manager Notification**: The departing employee’s manager will be notified once access is revoked.

### **5. Common Internal Tools & Systems**

The following are key tools used by Company K employees, along with general setup and access instructions:

#### **5.1 Microsoft Teams (Internal Communication)**

* **Purpose**: Used for internal communication, meetings, and collaboration.
* **Access**: Employees will automatically be added to Teams channels relevant to their department and projects.
* **Login**: Use Company K email and password to sign in.

#### **5.2 Jira or Asana (Project Management)**

* **Purpose**: Used for tracking project tasks, deadlines, and team collaboration.
* **Access**: Provided to employees in project management, IT, and operations roles.
* **Login**: Use Company K SSO (Single Sign-On) for authentication.

#### **5.3 Salesforce (CRM for Sales Team)**

* **Purpose**: Used for managing customer relationships, tracking sales leads, and reporting.
* **Access**: Sales team members and managers are granted access.
* **Login**: Salesforce account created by IT; login details provided upon access approval.

#### **5.4 GitHub/Bitbucket (Code Repository for IT and DevOps)**

* **Purpose**: Used by the IT and DevOps teams for managing code repositories and software development projects.
* **Access**: IT staff, developers, and DevOps engineers are granted access.
* **Login**: Integrated with Company K’s SSO for secure access.

#### **5.5 SAP (ERP System for Finance and Operations)**

* **Purpose**: Used for managing business operations, finance, supply chain, and inventory.
* **Access**: Finance, operations, and procurement departments.
* **Login**: SAP credentials provided by IT based on department role.

### **6. Security and Compliance**

#### **6.1 Multi-Factor Authentication (MFA)**

Company K enforces Multi-Factor Authentication (MFA) for all critical systems and tools to enhance security. Employees are required to authenticate using a second factor (e.g., SMS code, authentication app) in addition to their password.

#### **6.2 Data Security Guidelines**

All employees must follow Company K’s data security guidelines when accessing internal systems:

* Use strong, unique passwords.
* Avoid sharing login credentials.
* Report any suspicious activity or unauthorized access to IT immediately.
* Follow encryption and secure transmission protocols when dealing with sensitive data.

#### **6.3 Compliance with Non-Disclosure Agreements (NDAs)**

Employees granted access to internal tools must comply with Company K’s non-disclosure agreements, ensuring that no proprietary information is shared outside of authorized channels.

### **7. Contacting IT Support**

For any issues related to access, employees should contact IT support through the following channels:

* **IT Helpdesk Portal**: [IT Helpdesk Link]
* **Email**: it-support@companyk.com
* **Phone**: [IT Support Phone Number]