Kiteforge Industries

INFORMATION SECURITY POLICY & SOP

Subject: Employee Offboarding & Access Revocation

Version: 1.2

Owner: IT Security Department

Effective Date: October 2023

1. Information Security Policy

1.1 Purpose

The purpose of this policy is to ensure that Kiteforge Industries' information assets and systems are protected during and after the employee offboarding process. Proper access revocation is critical to preventing unauthorized access to sensitive data and maintaining the integrity of our security posture.

1.2 Scope

This policy applies to all employees, contractors, and third-party vendors at Kiteforge Industries (approx. 500-900 staff). It covers all company-issued devices, SaaS applications, internal networks, and physical access credentials.

1.3 Roles and Responsibilities

- **Human Resources (HR):** Responsible for notifying IT of all departures (voluntary or involuntary) immediately via the ticketing system and coordinating the exit interview.
- **IT Security/IT Ops:** Responsible for executing the technical revocation of access, wiping company hardware, and auditing account closures.
- **Department Managers:** Responsible for verifying the return of all physical assets and identifying any department-specific shared accounts or local access that must be revoked.
- **Legal:** Involved in cases of involuntary termination to ensure compliance with labor laws and preservation of data for legal hold if necessary.

1.4 Acceptable Use Highlights

Employees must adhere to the Kiteforge Acceptable Use Policy until their final minute of employment. Any attempt to export company data, delete files maliciously, or bypass security controls during the notice period will be treated as a major security incident.

1.5 Device Encryption

All Kiteforge laptops and mobile devices are protected by full-disk encryption (FileVault for macOS / BitLocker for Windows). Encryption keys are managed centrally by IT Security. Upon offboarding, devices must be returned in an encrypted state. No employee is authorized to decrypt a device prior to return.

1.6 Incident Reporting

Any suspicion of data exfiltration or unauthorized access during the offboarding window must be reported immediately to **security-incidents@kiteforge.com**. IT Security will initiate a forensic review of the departing user's activity logs if a red flag is raised.

> **Notice:** Failure to comply with these security protocols during offboarding may result in legal action or withholding of final severance where permitted by local law.

2. SOP: Employee Offboarding

This Standard Operating Procedure (SOP) ensures a consistent and secure transition when an employee leaves Kiteforge Industries.

Step 1: HR Ticket Initiation

HR creates a "Departure Ticket" in the IT Service Management (ITSM) portal. This must include the employee's name, ID, last working day, and termination type (Standard or Immediate).

Step 2: IT Checklist Activation

IT Security reviews the ticket and assigns an engineer. The engineer pulls the user's "Access Profile" which lists all assigned hardware and software licenses.

Step 3: SaaS and Identity Revocation

At 5:00 PM on the last day (or immediately for involuntary departures), IT disables the Primary Identity Provider (Okta/Azure AD) account. This automatically terminates access to Slack, Jira, Salesforce, and Email.

Step 4: Laptop Collection and Wipe

The laptop is collected. IT performs a "Cryptographic Wipe" of the drive. The hardware is inspected for physical damage and then moved to the "Pending Re-provisioning" inventory.

Step 5: Manager Verification

The manager completes a final sign-off form confirming all keys, badges, and department-specific assets have been recovered.

3. Governance

3.1 RACI Matrix

Activity	HR	IT	Mgr	Legal
Create Offboarding Ticket	A / R	I	C	I
Disable SaaS Accounts	I	A / R	I	-
Hardware Collection	C	I	A / R	-
Cryptographic Wipe	-	A / R	-	-
Physical Badge Retrieval	R	I	A	-

3.2 Revision History

Version	Date	Author	Description
1.0	Jan 2022	IT Security	Initial Draft
1.1	Mar 2023	Compliance	Added Device Encryption section
1.2	Oct 2023	IT Security	Updated for 500+ employee scale