# PERSONNEL SECURITY POLICY

For this policy, the following stakeholders may be involved with data gathering and review:

* Human Resources
* IT
* Security

What is the name of your company? (Replaces all the “Company” options)

|  |  |  |  |
| --- | --- | --- | --- |
| Version: | What is the version of this document? | Effective Date: | When does or did the policy become effective? |
| Owner and Title: | What is the name and title of the individual who owns this policy? | **Approver and Title:** | What is the name and title of the individual -typically, an executive - who approves this policy? |
| Last Review Date: | When was the last review date of this document? (If new document, enter N/A) | **Next Review Date:** | What is the next review date of this document? (Typically, a year after creation/last date) |

**Applicability**

This Policy applies to all Company employees, directors, and officers; any other individual or organization performing work for Company, including those employed by third parties, (collectively known as “Users”), all data and systems, including those employed by third parties, (collectively known as “Assets”); and business processes used by or supporting Company.

**Scope**

What is the physical scope of the policy? Choose from the drop-down options or enter custom answer)

Lucas – see options in the “Choose an item” drop down hereChoose an item.

**Target Audience**

What type of users does policy apply to? Choose from the drop-down options or enter custom answer)

Lucas – see options in the “Choose an item” drop down hereChoose an item.

**Purpose**

The Personnel Policy outlines Company responsibilities and expectations for users of Company assets, including third parties, during the employment lifecycle.

This Policy details Company’s requirements for:

* Educating and raising awareness with users on their roles and responsibilities for safeguarding Company assets.
* Managing disciplinary actions for users who violate Company policies and requirements.
* Ensuring Company compliance with applicable laws and regulations, to include. Which laws and regulations are applicable to your organization? If none, leave blank. If blank, remove the two words “to include”

# Key Points to Remember

* Users are made aware of their responsibilities to safeguard assets via awareness and training and agree to those responsibilities in Acceptable Use policy.
* Users receive reoccurring awareness training and users with more role-specific security functions and/or privileged access to sensitive assets receive enhanced trainings.
* Records of trainings are retained.
* Users agree to their responsibilities prior to gaining access.
* If users change roles, their access needs are reviewed.
* Terminated or suspended users (those departing for a temporary time) have their access decommissioned.
* A disciplinary process is in place to address users who deviate from the company policies.

**Policy Compliance**

This Policy shall take effect upon publication. Defined users of Company’s assets Select one: must, shall, will, should, may comply with the requirements outlined in this Policy.

Is there other legal content you would like to include? If none, leave blank.

**Policy Violation**

The Policy Owner Select one: must, shall, will, should, may be notified of material breaches of this Policy, whether intentional or inadvertent. Violation of these Policies Select one: must, shall, will, should, may be subject to disciplinary action, up to and including termination. Company retains discretion as to how to respond to violation of this Policy and shall undertake disciplinary process in accordance with all applicable laws and other legal requirements.

Is there other legal content you would like to include? If none, leave blank.

**Policy Exceptions**

Company Select one: must, shall, will, should, may grant exceptions to this Policy subject to written approval from the Company Who is the title who may approve exceptions? Exceptions granted Select one: must, shall, will, should, may not undermine the requirements set forth in this Policy.

Exception requests Select one: must, shall, will, should, may be submitted in writing to the Company Who is the title who may approve exceptions? with justification for the requested exception. Exception requests Select one: must, shall, will, should, may include potential risks of the exception and compensating controls to address residual risk.

Granted exceptions Select one: must, shall, will, should, may be documented and retained for the life of the exception. Exceptions Select one: must, shall, will, should, may be subject to review on a How frequently are granted exceptions reviewed? basis and potentially reassessed to ensure risk is not introduced to Company.

**Supplemental Information**

List documents and their location for relevant information If they have none, can be N/A. If more than one, can more lines be added?

Name of document Link or location

**Controls Alignment**

* **NIST CSF 2.0:** GV.RR-04, PR.AT-01, PR.AT-02
* **CIS Critical Security Controls:** 14.1, 14.2, 14.3

**POLICY**

1. **Roles and Responsibilities**

Formal job descriptions to include roles and responsibilities and related security expectations Select one: must, shall, will, should, may be documented and retained for How long are job descriptions retained for? Job descriptions Select one: must, shall, will, should, may be distributed to users upon hire and readily accessible afterwards.

1. **Agreement Signatures**

Users Select one: must, shall, will, should, may review and sign their acknowledgement of the Company What is the name of the agreement users are required to sign? This is typically “Acceptable Use” Policy and What is the name of the non-disclosure agreement users are required to sign? This is typically “Non Disclosure Agreement” prior to being granted logical and physical access to Company assets and facilities.

These signed Name of agreement in paragraph above Policy and name of agreement in paragraph above Select one: must, shall, will, should, may be retained for How long are they retained for?

1. **Security Education and Awareness**

Users Select one: must, shall, will, should, may receive a combination of training and other initiatives designed to raise awareness of their roles and responsibilities, as well as best practices for safeguarding Company assets.

Users with access to Company’s assets Select one: must, shall, will, should, may be required to receive security awareness training prior to being granted access. Users Select one: must, shall, will, should, may receive recurring security awareness trainings.

Users with access to Company assets designated with What are your sensitive assets classified as? Typically, they are labeled with Confidential, Sensitive, Internal Use Only classifications Select one: must, shall, will, should, may receive enhanced security training.

Users with specialized roles Select one: must, shall, will, should, may receive role-specific awareness and skills training.

Records of training conducted Select one: must, shall, will, should, may be retained for How long are training records retained for?

1. **Access**

Users Select one: must, shall, will, should, may be provided with access rights and permissions to Company assets that meet or exceed requirements in the Company Identity and Access Management Policy.

**4.1 New Users**

Users Select one: must, shall, will, should, may be granted access solely to Company assets required to perform their job duties and responsibilities (Need-to-Know).

Access to additional Company assets designated with What are your sensitive assets classified as? Typically, they are labeled with Confidential, Sensitive, and/or Internal Use Only classifications Select one: must, shall, will, should, may require Who are the title/s who can provide this approval to sensitive assets? written approval prior to be provisioned.

Records of provisioned access Select one: must, shall, will, should, may be retained for How long are provisioning records retained for?

**4.2 During Employment**

Prior to user role changes, the user’s access to Company assets Select one: must, shall, will, should, may be reviewed to ensure they are still required and updated as appropriate for Company assets designated with What are your sensitive assets classified as? Typically, they are labeled with Confidential, Sensitive, and/or Internal Use Only classifications.

Review of granted access permissions to Company assets designated with What are your sensitive assets classified as? Typically, they are labeled with Confidential, Sensitive, and/or Internal Use Only classifications Select one: must, shall, will, should, may be performed How frequently are privileged access permissions reviewed? Access permission reviews to non-sensitive Company assets Select one: must, shall, will, should, may be performed.

**4.3 Terminated Users**

General access for departing users Select one: must, shall, will, should, may bedisabled within What is the time window in which general access for departing users is disabled. Privileged access for departing select be ended within What is the time window in which privileged access for departing users is disabled.

User IDs for departing users Select one: must, shall, will, should, may beChoose one How are general user IDs disabled? deleted or deactivated on systems within What is the time window in which UserIDs for departing users is disabled. Privileged access for departing users Select one: must, shall, will, should, may beChoose one: How are privileged user IDs? deleted or deactivated on systems within What is the time window in which UserIDs for departing privileged users is disabled.

Users Select one: must, shall, will, should, may be required to return assigned Company assets and property.

**4.4 Suspended Users**

General access for temporarily departing users Select one: must, shall, will, should, may beended within What is the time window in which general access for temporarily departing users is disabled. Privileged access for departing users Select one: must, shall, will, should, mayended within What is the time window in which general access for temporarily departing privileged users is disabled.

User IDs for temporarily departing general users Select one: must, shall, will, should, may beChoose one How are general user IDs disabled? deleted or deactivated within What is the time window in which UserIDs for departing users is disabled? Privileged access for departing users Select one: must, shall, will, should, mayChoose one How are privileged user IDs disabled? deleted or deactivated within What is the time window in which UserIDs for departing privileged users is disabled.

Users Select one: must, shall, will, should, may be required to return assigned Company assets and property during their absence.

1. **Third Parties**

Designated third parties Select one: must, shall, will, should, may berequired to agree to, and meet or exceed, the requirements set forth in this Policy and other Company Policies.

The third party Select one: must, shall, will, should, may granted privileged access to their users only upon written approval by Company. Changes in access, including changes in roles and terminations, Select one: must, shall, will, should, may be communicated and approved in writing by Company.

An assessment Select one: must, shall, will, should, may be performed of the third party’s adherence to this Policy.

1. **Disciplinary Process**

A formal disciplinary process Select one: must, shall, will, should, may be in place to address user failure to comply with or violations of Company policies.

**Review**

This Policy Select one: must, shall, will, should, may be reviewed periodically (at least How often should this policy be reviewed? It is typically annually) and/or after any significant changes to Company’s business practices or processing environment(s), to ensure that the contents remain current and appropriate.

New revisions of the Policy Select one: must, shall, will, should, may be published.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version Number | Revision Type | Date: | Change Details |
| 1.0 | Original Issue | What date should be used for policy creation? | No Change |
| 1.1 | Review | What date should be used for the next review date of the policy? | What changes were made in this update? If none, state N/A. |

**END OF POLICY**