# PERSONNEL SECURITY POLICY

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

* Human Resources
* IT
* Security

|  |  |  |  |
| --- | --- | --- | --- |
| Version: | ${version} | Effective Date: | ${effectiveDate} |
| Owner and Title: | ${ownerTitle} | **Approver and Title:** | ${approverTitle} |
| Last Review Date: | ${lastReviewDate} | **Next Review Date:** | ${nextReviewDate} |

**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**

${scope}

**Target Audience**

${targetAudience}

**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 ${laws\_regulations}

# 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 ${select1} comply with the requirements outlined in this Policy.

${legal\_content}.

**Policy Violation**

The Policy Owner ${select2} be notified of material breaches of this Policy, whether intentional or inadvertent. Violation of these Policies ${select3} 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.

${legal\_content}.

**Policy Exceptions**

${company} ${select4} grant exceptions to this Policy subject to written approval from the ${company} ${title}. Exceptions granted ${select41} 1 not undermine the requirements set forth in this Policy.

Exception requests ${select5} be submitted in writing to the ${company} ${title} with justification for the requested exception. Exception requests ${select6} include potential risks of the exception and compensating controls to address residual risk.

Granted exceptions ${select7} be documented and retained for the life of the exception. Exceptions ${select8} be subject to review on a ${exceptionReviewed} basis and potentially reassessed to ensure risk is not introduced to ${company}.

**Supplemental Information**

${supplemental}

**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 ${select81} be documented and retained for ${jobRetained} Job descriptions ${select9} be distributed to users upon hire and readily accessible afterwards.

1. **Agreement Signatures**

Users ${select10} review and sign their acknowledgement of the ${company} ${agreementUsers} Policy and ${signName} prior to being granted logical and physical access to ${company} assets and facilities.

These signed ${nameAgreement} Policy and ${nameAgreement} ${select11} be retained for ${longRetained}

1. **Security Education and Awareness**

Users ${select12} 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 ${select13} be required to receive security awareness training prior to being granted access. Users ${select14} receive recurring security awareness trainings.

Users with access to ${company} assets designated with ${sensitiveAsset} classifications ${select15} receive enhanced security training.

Users with specialized roles ${select16} receive role-specific awareness and skills training.

Records of training conducted ${select17} be retained for ${longTrain}

1. **Access**

Users ${select18} 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 ${select19} 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 ${assetsClassified} classifications ${select51} require ${approvalSensitive} written approval prior to be provisioned.

Records of provisioned access ${select52} be retained for ${provisioningRetained}?

**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 ${assetsClassified} classifications.

Review of granted access permissions to ${company} assets designated with ${assetsClassified} classifications ${select20} be performed ${privilegedAccess} Access permission reviews to non-sensitive ${company} assets ${select21} be performed.

**4.3 Terminated Users**

General access for departing users ${select22} bedisabled within ${disabledTime}. Privileged access for departing ${select100} be ended within ${privilegedTime}.

User IDs for departing users ${select24} be${IDDisabled} on systems within ${IDTime}. Privileged access for departing users ${select25} be${privilegedId} on systems within ${idPrivilegedTime}.

Users ${select26} be required to return assigned ${company} assets and property.

**4.4 Suspended Users**

General access for temporarily departing users ${select27} be ended within ${generalAccessDisabled}. Privileged access for departing users ${select28} ended within ${generalAccessTime}.

User IDs for temporarily departing general users ${select29} be ${IDDisabled} within ${IDTime}? Privileged access for departing users ${select30} ${privilegedIdDisabled} within ${idPrivilegedTime}.

Users ${select31} be required to return assigned ${company} assets and property during their absence.

1. **Third Parties**

Designated third parties ${select32} berequired to agree to, and meet or exceed, the requirements set forth in this Policy and other ${company} Policies.

The third party ${select33} granted privileged access to their users only upon written approval by ${company}. Changes in access, including changes in roles and terminations, ${select34} be communicated and approved in writing by ${company}.

An assessment ${select341} be performed of the third party’s adherence to this Policy.

1. **Disciplinary Process**

A formal disciplinary process ${select35} be in place to address user failure to comply with or violations of ${company} policies.

**Review**

This Policy ${select36} be reviewed periodically (at least ${oftenReviewed}) 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 ${select37} be published.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version Number | Revision Type | Date: | Change Details |
| 1.0 | Original Issue | ${dateCreation} | No Change |
| 1.1 | Review | ${nextReviewDate} | ${updateChanged} |

**END OF POLICY**