# PERSONNEL SECURITY POLICY

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

* Human Resources
* IT
* Security

|  |  |  |  |
| --- | --- | --- | --- |
| Version: | \_\_\_\_\_\_ | Effective Date: | \_\_\_\_\_\_ |
| Owner and Title: | \_\_\_\_\_\_ | **Approver and Title:** | \_\_\_\_\_\_ |
| Last Review Date: | \_\_\_\_\_\_ | **Next Review Date:** | \_\_\_\_\_\_ |

**Applicability**

This Policy applies to all \_\_\_\_\_\_ employees, directors, and officers; any other individual or organization performing work for \_\_\_\_\_\_, 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 \_\_\_\_\_\_.

**Scope**

\_\_\_\_\_\_

**Target Audience**

\_\_\_\_\_\_

**Purpose**

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

This Policy details \_\_\_\_\_\_’s requirements for:

* Educating and raising awareness with users on their roles and responsibilities for safeguarding \_\_\_\_\_\_ assets.
* Managing disciplinary actions for users who violate \_\_\_\_\_\_ policies and requirements.
* Ensuring \_\_\_\_\_\_ compliance with applicable laws and regulations, 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 \_\_\_\_\_\_ policies.

**Policy Compliance**

This Policy shall take effect upon publication. Defined users of \_\_\_\_\_\_’s assets \_\_\_\_\_\_ comply with the requirements outlined in this Policy.

\_\_\_\_\_\_.

**Policy Violation**

The Policy Owner \_\_\_\_\_\_ be notified of material breaches of this Policy, whether intentional or inadvertent. Violation of these Policies \_\_\_\_\_\_ be subject to disciplinary action, up to and including termination. \_\_\_\_\_\_ 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.

\_\_\_\_\_\_.

**Policy Exceptions**

\_\_\_\_\_\_ \_\_\_\_\_\_ grant exceptions to this Policy subject to written approval from the \_\_\_\_\_\_ \_\_\_\_\_\_. Exceptions granted \_\_\_\_\_\_ 1 not undermine the requirements set forth in this Policy.

Exception requests \_\_\_\_\_\_ be submitted in writing to the \_\_\_\_\_\_ \_\_\_\_\_\_ with justification for the requested exception. Exception requests \_\_\_\_\_\_ include potential risks of the exception and compensating controls to address residual risk.

Granted exceptions \_\_\_\_\_\_ be documented and retained for the life of the exception. Exceptions \_\_\_\_\_\_ be subject to review on a \_\_\_\_\_\_ basis and potentially reassessed to ensure risk is not introduced to \_\_\_\_\_\_.

**Supplemental Information**

\_\_\_\_\_\_

**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 \_\_\_\_\_\_ be documented and retained for \_\_\_\_\_\_ Job descriptions \_\_\_\_\_\_ be distributed to users upon hire and readily accessible afterwards.

1. **Agreement Signatures**

Users \_\_\_\_\_\_ review and sign their acknowledgement of the \_\_\_\_\_\_ \_\_\_\_\_\_ Policy and \_\_\_\_\_\_ prior to being granted logical and physical access to \_\_\_\_\_\_ assets and facilities.

These signed \_\_\_\_\_\_ Policy and \_\_\_\_\_\_ \_\_\_\_\_\_ be retained for \_\_\_\_\_\_

1. **Security Education and Awareness**

Users \_\_\_\_\_\_ receive a combination of training and other initiatives designed to raise awareness of their roles and responsibilities, as well as best practices for safeguarding \_\_\_\_\_\_ assets.

Users with access to \_\_\_\_\_\_’s assets \_\_\_\_\_\_ be required to receive security awareness training prior to being granted access. Users \_\_\_\_\_\_ receive recurring security awareness trainings.

Users with access to \_\_\_\_\_\_ assets designated with \_\_\_\_\_\_ classifications \_\_\_\_\_\_ receive enhanced security training.

Users with specialized roles \_\_\_\_\_\_ receive role-specific awareness and skills training.

Records of training conducted \_\_\_\_\_\_ be retained for \_\_\_\_\_\_

1. **Access**

Users \_\_\_\_\_\_ be provided with access rights and permissions to \_\_\_\_\_\_ assets that meet or exceed requirements in the \_\_\_\_\_\_ Identity and Access Management Policy.

**4.1 New Users**

Users \_\_\_\_\_\_ be granted access solely to \_\_\_\_\_\_ assets required to perform their job duties and responsibilities (Need-to-Know).

Access to additional \_\_\_\_\_\_ assets designated with \_\_\_\_\_\_ classifications \_\_\_\_\_\_ require \_\_\_\_\_\_ written approval prior to be provisioned.

Records of provisioned access \_\_\_\_\_\_ be retained for \_\_\_\_\_\_?

**4.2 During Employment**

Prior to user role changes, the user’s access to \_\_\_\_\_\_ assets Select one: must, shall, will, should, may be reviewed to ensure they are still required and updated as appropriate for \_\_\_\_\_\_ assets designated with \_\_\_\_\_\_ classifications.

Review of granted access permissions to \_\_\_\_\_\_ assets designated with \_\_\_\_\_\_ classifications \_\_\_\_\_\_ be performed \_\_\_\_\_\_ Access permission reviews to non-sensitive \_\_\_\_\_\_ assets \_\_\_\_\_\_ be performed.

**4.3 Terminated Users**

General access for departing users \_\_\_\_\_\_ bedisabled within \_\_\_\_\_\_. Privileged access for departing \_\_\_\_\_\_ be ended within \_\_\_\_\_\_.

User IDs for departing users \_\_\_\_\_\_ be\_\_\_\_\_\_ on systems within \_\_\_\_\_\_. Privileged access for departing users \_\_\_\_\_\_ be\_\_\_\_\_\_ on systems within \_\_\_\_\_\_.

Users \_\_\_\_\_\_ be required to return assigned \_\_\_\_\_\_ assets and property.

**4.4 Suspended Users**

General access for temporarily departing users \_\_\_\_\_\_ be ended within \_\_\_\_\_\_. Privileged access for departing users \_\_\_\_\_\_ ended within \_\_\_\_\_\_.

User IDs for temporarily departing general users \_\_\_\_\_\_ be \_\_\_\_\_\_ within \_\_\_\_\_\_? Privileged access for departing users \_\_\_\_\_\_ \_\_\_\_\_\_ within \_\_\_\_\_\_.

Users \_\_\_\_\_\_ be required to return assigned \_\_\_\_\_\_ assets and property during their absence.

1. **Third Parties**

Designated third parties \_\_\_\_\_\_ berequired to agree to, and meet or exceed, the requirements set forth in this Policy and other \_\_\_\_\_\_ Policies.

The third party \_\_\_\_\_\_ granted privileged access to their users only upon written approval by \_\_\_\_\_\_. Changes in access, including changes in roles and terminations, \_\_\_\_\_\_ be communicated and approved in writing by \_\_\_\_\_\_.

An assessment \_\_\_\_\_\_ be performed of the third party’s adherence to this Policy.

1. **Disciplinary Process**

A formal disciplinary process \_\_\_\_\_\_ be in place to address user failure to comply with or violations of \_\_\_\_\_\_ policies.

**Review**

This Policy \_\_\_\_\_\_ be reviewed periodically (at least \_\_\_\_\_\_) and/or after any significant changes to \_\_\_\_\_\_’s business practices or processing environment(s), to ensure that the contents remain current and appropriate.

New revisions of the Policy \_\_\_\_\_\_ be published.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version Number | Revision Type | Date: | Change Details |
| 1.0 | Original Issue | \_\_\_\_\_\_ | No Change |
| 1.1 | Review | \_\_\_\_\_\_ | \_\_\_\_\_\_ |

**END OF POLICY**