**PERSONNEL SECURITY**

POLICY

Contents

# Policy

****

|  |  |  |  |
| --- | --- | --- | --- |
| Policy Title | Personnel Security | | |
| Version: | Click to enter text | **Effective Date:** | Enter date |
| Owner and Title: | Click to enter text | **Approver and Title:** | Click to enter text |
| Last Review Date: | Click to enter text | **Next Review Date:** | Enter 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: | Choose an item. | Specifics: | Choose an item. |
| Target Audience: | Choose an item. | **Specifics:** | Choose an item. |
| Audience Type: | Choose an item. | **Specifics:** | Choose an item. |

**Purpose**

The Personnel Policy outlines Company approved requirements for assigning and managing requirements and expectations for users, 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 add custom list.

**Policy Compliance**

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

Add relevant Legal jargon here

**Policy Violation**

The Policy Owner select be notified of material breaches of this Policy, whether intentional or inadvertent. Violation of these Policies select 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.

Add relevant Legal jargon here

**Policy Exceptions**

Company select grant exceptions to this Policy subject to written approval from the Company Title/s. Exceptions granted select not undermine or conflict with the requirements set forth in this Policy.

Exception requests select be submitted in writing to the Company Title/s with justification for the requested exception. Exception requests select include potential risks of the exception and compensating controls to address any residual risk.

Granted exceptions select be documented and retained for the life of the exception. Exceptions select be subject to review and potential reassessment to ensure risk is not introduced to Company.

**Supplemental Information**

Name of document Link or location

Name of document Link or location

Name of document Link or location

Name of document Link or location

**POLICY**

1. **Roles and Responsibilities**

Formal job descriptions to include roles and responsibilities and related security expectations select be documented and retained select. Job descriptions select be distributed to users upon hire and select afterwards.

1. **Acceptable Use and Non-Disclosure Agreement**

Users select review and sign their acknowledgement of the Company select Policy and select prior to being granted select access to Company select

The signed select Policy and select select be retained select.

1. **Security Education and Awareness**

Users select 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 select select be required to receive security awareness training prior to being granted select access. Users select receive recurring security awareness trainings.

Users with access to Company assets designated with Select, Select, and Select classifications select receive enhanced security training.

Users with specialized role required awareness select receive role-specific awareness and skills training.

Records of training conducted select be retained select.

1. **Access**

Users select be provided with access rights and permissions to Company select that meet or exceed requirements in the Company select Policy.

**4.1 New Users**

Users select 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 Select, Select, and Select classifications select require select written approval prior to be provisioned.

Records of provisioned access select be retained select.

**4.2 During Employment**

Prior to user role changes, the user’s access to Company assets select be reviewed to ensure they are still required and updated as appropriate for Company assets designated with Select, Select, and Select classifications.

Review of granted access permissions to Company assets designated with Select, Select, and Select classifications select be performed select. Access permission reviews to non-sensitive Company assets select performed.

**4.3 Terminated Users**

General access for departing users select beended select. Privileged access for departing select be ended select.

User IDs for departing general users select beselect select. Privileged access for departing users select beselect select.

Users select be required to return assigned Company assets and property.

**4.4 Suspended Users**

General access for temporarily departing users select beended select. Privileged access for departing users selectended select.

User IDs for temporarily departing general users select beselect select. Privileged access for departing users selectselect select.

Users select be required to return assigned Company assets and property during their absence.

1. **Third Parties**

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

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

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

1. **Disciplinary Process**

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

**Review**

This Policy select be reviewed periodically (at least enter period of time) 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 be published.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version Number | Revision Type | Date: | Change Details |
| 1.0 | Original Issue | Enter date | No Change |
| 1.1 | Annual Review | Enter date |  |

**END OF POLICY**

# Appendix A: Key Points to Remember from this Policy

* 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.

# Appendix B: Typical Stakeholders for this Policy

The following stakeholders may be involved in gathering data and providing review for this Policy:

* Human Resources
* IT
* Security

# Appendix C: Information Gathering (by Function)

For instructions on how to choose the **Term to Select** in the tables below, please refer to the **Quick Start Guide for Policies.** These terms are used through the Policy to identify the level of compliance needed with each control.

## Human Resources:

|  |  |  |
| --- | --- | --- |
| Section | Question | Term to Select |
| 1. | Are formal job descriptions created which include roles and responsibilities and related security expectations and are they retained? | select |
| 3. | Do 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? | select |
| 3. | Do users with access to the network and facilities required to receive security awareness training prior to being granted this access? | select |
| 3. | Do users receive recurring security awareness trainings? | select |
| 3. | Do users with privileged access to sensitive assets receive enhanced security training? | select |
| 3. | Do users with specialized role required awareness receive role-specific awareness and skills training? | select |
| 3. | Are records of trainings conducted retained and kept updated? | select |
| 3. | How long are training records retained for? | select |
| 4.2 | When users change roles, is access reviewed to ensure the access is still required and updated as appropriate for sensitive assets? | select |
| 4.3 | How quickly is general access for departing users terminated? | select |
| 4.3 | How quickly is privileged access for departing users terminated? | select |
| 4.3 | Are users typically required to return assigned assets and property? | select |
| 4.4 | Is access for suspended or temporarily away general users ended? | select |
| 4.4 | How quickly is access for suspended general users decommissioned? | select |
| 4.4 | Are suspended users typically required to return assigned assets and property during their absence? | select |
| 6. | Is a formal disciplinary process in place to address user failure to comply with or violations of Company policies? | select |

## IT and/or Security:

|  |  |  |
| --- | --- | --- |
| Section | Question | Term to Select |
| 1. | Are formal job descriptions created which include roles and responsibilities and related security expectations and are they retained? | select |
| 1. | Are job descriptions distributed to users upon hire and are available afterwards? | select |
| 1. | How long are job descriptions retained for? | select |
| 2. | Do users review and sign their acknowledgement of the Acceptable Use policy and NDA prior to being granted both logical and physical access? | select |
| 2. | Are these signed documents retained and for how long of a period? | select |
| 3. | Do 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? | select |
| 3. | Do users with access to the network and facilities required to receive security awareness training prior to being granted this access? | select |
| 3. | Do users receive recurring security awareness trainings? | select |
| 3. | Do users with privileged access to sensitive assets receive enhanced security training? | select |
| 3. | Do users with specialized role required awareness receive role-specific awareness and skills training? | select |
| 3. | Are records of trainings conducted retained and kept updated? | select |
| 3. | How long are training records retained for? | select |
| 4. | Are users typically provided with logical and physical access rights and permissions to electronic and physical assets? | select |
| 4. | Does the level of access provided meet or exceed the requirements in the Identity and Access Management Policy? | select |
| 4.1 | Are new users typically granted access solely to assets required to perform their job duties and responsibilities (Need-to-Know)? | select |
| 4.1 | Does access to additional sensitive assets typically require written approval prior to be provisioned? | select |
| 4.1 | What level of leadership is required to approve the access to sensitive assets? | select |
| 4.1 | Are records of provisioned access retained? | select |
| 4.1 | How long are provisioned access records retained for? | select |
| 4.2 | When users change roles, is access reviewed to ensure the access is still required and updated as appropriate for sensitive assets? | select |
| 4.2 | Are reviews of granted access permissions to sensitive assets performed? | select |
| 4.2 | How often are reviews of granted access permissions to sensitive assets performed? | select |
| 4.2 | Are access permission reviews to non-sensitive assets performed? | select |
| 4.3 | How quickly is general access for departing users terminated? | select |
| 4.3 | How quickly is privileged access for departing users terminated? | select |
| 4.3 | How are user IDs for general users decommissioned? | select |
| 4.3 | How quickly are user IDs for general users decommissioned? | select |
| 4.3 | How are user IDs for departing privileged users terminated? | select |
| 4.3 | How quickly are user IDs for privileged users decommissioned? | select |
| 4.3 | Are users typically required to return assigned assets and property? | select |
| 4.4 | Is access for suspended or temporarily away general users ended? | select |
| 4.4 | How quickly is access for suspended general users decommissioned? | select |
| 4.4 | Are user IDs for suspended or temporarily away privileged users ended? | select |
| 4.4 | How quickly are user IDs for suspended privileged users decommissioned? | select |
| 4.4 | Are suspended users typically required to return assigned assets and property during their absence? | select |
| 5. | Do designated third parties typically agree to, and meet or exceed, the requirements set forth in this Policy and other Company Policies? | select |
| 5. | Is written approval required before the third party grants privileged access to their users? | select |
| 5. | Are third party changes in access required to be approved prior to being granted? | select |
| 5. | Are assessments performed of the third party’s adherence to this Policy? | select |
| 6. | Is a formal disciplinary process in place to address user failure to comply with or violations of Company policies? | select |