**U05A1 – Personnel Security Policy**

**Chris Misch**

School of Business, Technology, and Health Care Administration, Capella University

IT4076: Security Management and Policies

Stuart McCubbrey

May 2023

1. **Overview**

The personnel security policy has been created to ensure the protection of sensitive information throughout the employment lifecycle, including pre-employment, during employment, and post-employment phases.

* 1. **Purpose**

The purpose of this policy is to establish controls that safeguard sensitive information collected from employees during their employment lifecycle These controls aim to ensure the safety and compliance of the hospital’s security policy, as well as relevant rules and regulations.

* 1. **Scope**

This policy applies to all employees, volunteers, and employee applicants of High Class Healthcare. It also extends to Human Resources and any person responsible for the handling of employee data during the on-boarding, off-boarding, and continued employment processes.

1. **Policy**

The personal security policy is based on the following pillars: screening, contracts, security policy acknowledgement, security education, monitoring, and termination procedures.

The Human Resources (HR) and legal departments will conduct background checks and verify the information provided by prospective applicants. As part of the onboarding process, the HR department will provide security training to each new employee. All data collected during the pre-employment, during employment, and post-employment will adhere to the guidelines outlined in NIST SP800-53R.5, Security and Privacy Controls for Information Systems and Organizations.

In the event where more than 50 people will be laid off High Class Healthcare will provide notice to the affected employees in compliance with the Worker Adjustment and Retraining Notification (WARN) Act.

* 1. **Pre-Employment:**

1. Resumes will be subject to fact checking as per each hiring manager.
2. Background checks and drug screenings will be performed on individuals selected for open positions.
3. Logs will be created and maintained and audited on all employees who have access to electronically stored data.
4. Review and update position risk designations no less than every 6 months but no longer than 12 months.
   1. **During Employment:**
5. Employees must ensure the secure and confidential handling of patient Personally Identifiable Information (PII) and Protected Health Information (PHI), refraining from sharing such information with unauthorized parties.
6. Drug Screens may be required in the event of a change in title, position, or transfer to a different department.
7. Random drug screenings may be conducted periodically.
   1. **Post-Employment**
8. Upon providing notice of resignation, employees will have their logs monitored until their last day of employment.
9. Within 48 hours after the employee’s last day, their single sign on access must be deactivated from accessing company data, applications, and devices. However, email access may be permitted up to 7 days post-employment.
10. All equipment and devices loaned to employees must be returned on their last day of employment.
11. Exit interviews will be conducted on exiting employees. These interviews will be done in person but in the case, this is not possible a zoom meeting may be set up. (NIST PR.AT-1 Personnel Security Policy)
12. Notify HR and the head of each department of which the employee had worked in, for, or along side within 48 hours before termination and no longer than 24 hours after termination.
13. **Access Control**
14. Data that is used, created, maintained, or accessed by an employe will be subject to security restrictions outlined in the Access Control Policy which defines authorization levels for employees, departments, and groups.
15. Badges and access cards will be issued to new hires on their first day on the job and collected on their last scheduled working day.
16. Access to data will be restricted or denied according to position, need, and authority according to Access Control policy.
17. **Information Security** 
    1. Personal data pertaining to individual employees will be encrypted and held off site and for no less than 1 year, according to 2023 HR Retention requirements.
    2. Data at rest and in transit will follow the standards according to Federal Information Processing Standard (FIPS) confidentiality of information.
    3. Information and records data are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. (PR.DS)
    4. Personal devices used as a part of the job must be scrubbed of any data owned, used, or accessed by High Class Healthcare.
    5. Employees may have access to their own records by following the data request policy which outlines how to request sensitive data.
18. **Training and Awareness**
19. Exiting employees must be notified of all applicable, legally binding post-employment requirements for the protection of information.
20. Terminated employees will sign an acknowledgement of post-employment requirements as directed by Counsel and HR.
21. Security training for employees will be conducted during the on-boarding process and as soon as 6 months but no later than 12 months from last retraining.
22. **Incident Reporting and Response**
23. In the event of an incident in handling personnel security HR and IT security must be notified immediately.
24. The Incident Response Policy shall be followed according to the nature of the incident.
25. Employees caught up in an incident shall be monitored for a time specified between HR and IT security.
26. **Policy Compliance**

All employees must adhere to this personnel security policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. This also may include civil and criminal penalties, non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties. (PR.AC)

1. **Related Standards, Policies, and Processes**

This policy has used the National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-53r.5 – PR.AT-1 Awareness and Training Personal Security Policy, PR.DS Data Security, FIPS. Regulations of PII and PHI, are adhered to follow HIPAA regulations and WARN act. Employee hiring, retention, and dismissal follow FCRA, EEOC and 2023 HR Record of Retention Guidelines. All other parts of the policy follow current security policies created for High Class Healthcare including Acceptable Use Policy, Compliance Policy, Privacy Policy, Incident Response Policy, and Access Control Policy.

1. **Definitions and Terms**

PR.DS – Information and records data are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.

PR.AC – Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.

WARN – Worker Adjustment and Retraining Notification Act.

CEO – Chief Executive Officer

FIPS – Federal Information Processing Standards.

1. **Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Revision Date | Summary of Changes | Approval |
| 1.0 | 05/13/2023 | Creation of new policy | Mark Moneybags, CEO |

1. **Resources**

Lineman, D. (2012). The Six Pillars of Personnel Security Policy. *Information Shield*. https://informationshield.com/2012/12/03/the-six-pillars-of-personnel-security-policy/

SecureScan. (2023). 2023 HR Record Retention Guidelines. *SecureScan*. <https://www.securescan.com/articles/document-scanning/hr-record-retention-guidelines/>

*Information Security Policy Template | HealthIT.gov*. (n.d.). https://www.healthit.gov/resource/information-security-policy-template