HR POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/HRP/012/1.0
Security Classification	Confidential
Date Issued	30-Jul-2025
Version	1.0
Project Name	NA
Author	AJ KHAN

VERSION HISTORY / CHANGE HISTORY

Version	Date Issued	Issued to	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

REVIEWERS

Version	Review Date	Reviewed By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

APPROVERS

Version	Date Approved	Approved By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

DISTRIBUTION LIST

Date	Name / Distribution List	Comments
30-Jul-2025	Customer_DL_ABC	Published to Customer ABC

DOCUMENT CONTROL PAGE

RELATED DOCUMENTS

DOC_ID	DOC Version#	DOC Link	Comments
SCG/BASEINS/005/1.0			Base Template Instructions
SCG/PXF/008/1.0			Policy Exception Form
SCG/S2RAS/113/1.0			SOC2 Asset Scope

CONFIDENTIALITY STATEMENT

This document is the exclusive property of [SecureCyberGates]. This document contains proprietary and confidential information. Duplication, Redistribution, or use, in whole or in part, in any form, requires consent of [SecureCyberGates].

[SecureCyberGates] may share this document with auditors under non-disclosure agreements [NDA] to demonstrate Security Audit requirement compliance.

Contents

1) Objective

Our HR Management Program serves as guidance for ensuring effective human resource management practices throughout [SecureCyberGates]. All employees are expected to adhere to the guidelines outlined in this policy. It is important to note that this HR Policy may not cover every possible scenario. If you are unsure how the standards or guidelines apply in a given situation, please seek guidance from the HR Manager or relevant department heads.

Each individual is responsible for ensuring compliance with these guidelines, and all stakeholders will be held accountable for upholding their commitments to this HR Policy.

2) Roles &Responsibilities

Roles	Responsibilities
CISO / Security Team	Review and Audit HR Policy.
HR Team	Overseeing the implementation and enforcement of this policy.Create, Manage, Monitor, Maintain, Audit "HR" Policy.
BU Heads or Project Managers	Ensuring that employees under their supervision comply with this policy. [Review HR Policy]
Employees / Contractors	1. Read this HR Policy 2. Ask questions / Provide Feedbacks 3. Report possible or actual violations of this HR Policy.

3) Scope

This Policy applies to anyone employed by or conducting business for [SecureCyberGates], including:

- All employees
- Management and company owners
- External business partners who act on [SecureCyberGates]'s behalf or in our interest as Third Party Representatives

4) HR Management Program

4.1) Objective

The objective of the HR Management Program is to develop, implement, and govern processes and documentation to facilitate effective human resource management practices in [SecureCyberGates].

4.2) Standard

[SecureCyberGates] is committed to implementing the following standard practices in HR management:

- Conducting a formal risk assessment at least annually and upon significant changes to the corporate environment.
- Identifying critical HR assets, including personnel data and organizational resources.
- Evaluating the effectiveness of existing HR safeguards and identifying potential threats and vulnerabilities.
- Reviewing HR processes, including recruitment, onboarding, performance management, and employee relations, to ensure compliance with internal policies and external regulations.
- Assigning responsibility for validating HR controls and monitoring their effectiveness.

4.3) Guidelines

The HR Management Program of [SecureCyberGates] adheres to the following guidelines:

- Utilizes industry-recognized practices to ensure effective HR management.
- Conducts formal risk assessments annually and upon significant changes to the corporate environment.
- Identifies critical assets, current safeguards, threats, and vulnerabilities.
- Reviews processes involving sensitive data handling.
- Assigns responsibility to validate HR controls.

5) Procedures

Control Activity: In-house HR Department along with Employee Training , Security and IT team.

- Develops and delivers Information Security Awareness Training programs to educate employees on information security best practices, including access control, data protection, and incident response.
- Implements Access Control measures, such as user authentication mechanisms, role-based access controls, and privileged access management, to enforce least privilege principles and restrict unauthorized access to sensitive information.
- Implements technical controls, such as encryption, data loss prevention (DLP) tools, and secure file transfer protocols, to protect sensitive data from unauthorized access, disclosure, or loss.
- Enforces BYOD Policy requirements, including device registration, security configuration, and remote wipe capabilities, to mitigate the risks associated with the use of personal devices for work purposes.
- Establishes Incident Response Procedures to ensure timely detection, reporting, assessment, and mitigation of security incidents or breaches, including notification to affected parties and regulatory authorities as required.

- Implements Physical Security Measures, such as access controls, surveillance cameras, and alarm systems, to protect company facilities, equipment, and assets from unauthorized access, theft, or damage.
- Conducts regular audits and assessments to evaluate compliance with HR policies and procedures, identify gaps or deficiencies, and implement corrective actions as necessary.
- Establishes a process for monitoring and enforcing compliance with HR policies, including disciplinary actions

5.1) Employee & Background Verification

[SecureCyberGates] adheres to scrupulous verification of candidates prior to letter of offer and onboarding. Human Resources require the candidates to submit proof of their identification. All Malaysian hires need to submit a copy of their National Registration Identity Card (NRIC). Foreign nationals need to submit a copy of their passport and visa page if relevant.

[SecureCyberGates]'s Human Resources processes a meticulous background verification to ensure there are no false claims or fabrications with the potential new hire. Educational certificates (High school and later), pay slips for the last three months, two references are required, if the applicant has prior work experience, then 1 from previous direct reporting manager and 1 from a peer or subordinate. If the applicant has no prior working experience, then references from their educational institutions are required before offer and onboarding. The records received are verified and copies are stored for future reference. The references provided are contacted by Human Resources and questions relevant to the candidate's role, skills, nature and conduct are inquired for and noted for further assessment. A CTOS [Credit Score Reporting Agency in Malaysia] check is conducted on applicants to understand whether the applicant owns any businesses outside of employment with [SecureCyberGates] and whether there are any points of concern on applicant's credit history.

5.2) Terms and Conditions of Employment/Contracting

Contractual agreements clearly state the responsibilities of employees, contractors, and the organization regarding information security, including:

- Signing confidentiality or non-disclosure agreements prior to accessing sensitive information
- Legal responsibilities and rights related to data protection, intellectual property, etc.
- Responsibilities for classifying and managing information assets
- Procedures for handling information from external parties
- Responsibilities for handling personal information
- Security responsibilities extending beyond the organization's premises and working hours

- Disciplinary actions for disregarding security requirements job function.
- Relevant security responsibilities continue for a defined period after termination of employment or contract.

5.3) Information security awareness, education and training

All employees, contractors, and relevant third parties receive appropriate security awareness education, training, and regular updates on organizational policies and procedures relevant to their roles.

5.4) Disciplinary process

Formal disciplinary processes are in place and communicated to employees and contractors. These processes apply to information security breaches or policy violations.

5.5) Termination or change of employment responsibilities

All employees are bound by a confidentiality clause that they have to adhere to after termination as well. It is agreed to maintain strict confidentiality of company information, client information and vendor information.

The procedures below where applicable have to be completed by every employee prior to their last day of employment at [SecureCyberGates].

1. Deletion of listed items from personal devices
    a. Company software
    b. Virtual Machines used for development, testing, training or other use
    c. Company documentation
    d. Company source code
    e. Company related correspondence, including email, proposals, pricing
2. Remove Email Access/ App from mobile device
3. Return of company notebook, notebook bag and notebook charger
4. Return of access card
5. Return of business card
6. Return of medical insurance card
7. Return of parking card
8. Return of office keys
9. Return of company documentation, books, DVDs etc.

The full exit checklist is verified by the employee’s Reporting manager or by a member from HR.

5.6) Access Management

Access rights to information assets and information processing facilities are granted based on the principles of least privilege and need-to-know.

Access rights are removed or adjusted upon termination or change of employment/contract, considering factors such as:

- Reason for termination/change (initiated by the individual or organization)
- Current responsibilities of the individual
- Sensitivity of the accessible assets

5.7) Personnel Transfers and Changes

Information security responsibilities and duties are clearly defined and communicated when personnel are transferred or change roles within the organization.

5.8) Remote Working

Security requirements for remote working, such as the use of secure communication channels, access controls, and data protection measures, are clearly defined and communicated.

5.9) Third-Party Personnel

Security requirements and responsibilities for third-party personnel with access to the organization's information assets are clearly defined and documented in contractual agreements

5.10) Onboarding and Offboarding

Onboarding processes for new employees or contractors include provisioning access, security training, and other security-related activities.
Offboarding processes for personnel leaving the organization include revoking access, handling data and assets, and other security-related activities.

5.11) Segregation of Duties

Critical tasks and responsibilities are divided among multiple individuals to prevent conflicts of interest and reduce the risk of fraud or unauthorized activities.

5.12) Clean Desk and Clear Screen

Guidelines for a clean desk and clear screen policy are included to ensure that physical documents and computer screens are secured when not in use.

5.13) Acceptable Use

An acceptable use policy is referenced or incorporated, outlining the appropriate and permissible use of the organization's information assets, such as computer systems, networks, and data storage devices.

5.14) Security Incident Reporting

Employees are required to report security incidents or suspected incidents promptly, and reporting procedures are outlined.

5.15) Performance Evaluation and Monitoring

Adherence to security policies and procedures is evaluated as part of employee and contractor performance evaluations and ongoing monitoring.

6) Employee Training and Awareness

6.1) All [SecureCyberGates] employees SHOULD undergo training and assessment on this policy during their initial induction [Onboarding].

6.2) Security team to conduct periodic trainings **ATLEAST ONCE** a year.

7) Compliance and Monitoring

7.1) Compliance with this policy is **MANDATORY**. Employees violating this policy will be subject to disciplinary action up to and including termination.

7.2) Third-party users, contractors, and vendors who **FAIL** to comply with this policy may have their access to [SecureCyberGates]systems and networks revoked or suspended until compliance is achieved. Repeated or severe violations may result in the termination of their contracts or business relationships with [SecureCyberGates].

7.3) Periodic Audits and Assessments : [SecureCyberGates]'s HR department, in collaboration with the Information Security team, will conduct periodic audits and assessments to evaluate compliance with this HR policy.

8) Escalation Matrix

8.1) In case of any policy violations issues, the following escalation structure shall be followed to ensure timely resolution and appropriate accountability:

Level	Role	Contact
Level 1	Team Lead /Reporting Manager	First-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 2	Group Manager / Senior Managers	Second-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 3	HR	Final-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]

8.2) Employee SHOULD provide sufficient evidences and details , Clear description of the issue.

8.3) Security team to define issue severity and proper SLA for issue resolution as per severity.

9) Policy Exceptions

9.1) There may be requirements where Employee needs policy exception for legitimate reasons, In such cases, employee should follow POLICY EXCEPTIONS template and approval process. **[Kindly refer Policy exception form [Document ID SCG/PXF/008/1.0]]**

10) Policy Review and Updates

10.1) This HR policy shall be periodically reviewed **[Atleast Once in a YEAR]**and updated to ensure its effectiveness, relevance, and alignment with [SecureCyberGates]objectives,legal requirements and industry best practices.

10.2) Feedback from employees, stakeholders, and external audits shall be solicited and considered for continuous improvement of the policy and associated procedures.

10.3) Regular audits and inspections shall be conducted to assess compliance with this policy and associated procedures, with non-conformances addressed through corrective actions and preventive measures.

10.4) Any updates or revisions to this policy will be communicated to all employees and relevant stakeholders through appropriate channels. Employees are responsible for familiarizing themselves with the latest version of the policy and adhering to its requirements.

11) Conclusion

[SecureCyberGates]is committed to maintaining the highest standards for Employee and HR security. Every employee plays a crucial role in safeguarding confidential information, and their diligence and cooperation are essential for the successful implementation of this policy.

THANKYOU!
FOR CYBER-SECURITY RELATED UPDATES, KINDLY FOLLOW BELOW PAGES…

https://www.linkedin.com/in/aj57/
https://www.linkedin.com/company/securecybergates
https://securecybergates.com/services
https://www.youtube.com/@SecureCyberGates
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com