Personnel Security and Awareness Training Policy

Purpose

The purpose of the (Company) Personnel Security and Awareness Training Policy is to ensure that all personnel with access to (Company) **Information Resources** are adequately vetted, qualified, and trained according to their role.

Audience

The (Company) Personnel Security and Awareness Training Policy applies to all individuals responsible for hiring, onboarding, offboarding, and training of personnel given access to (Company) **Information Resources**.

Contents

[General](#_Toc49848244)

[Background Checks](#_Toc49848245)

[Training and Awareness](#_Toc49848246)

Policy

General

* For all roles within (Company), the hiring process should ensure the candidate has the necessary competence to perform the role and can be trusted to take on the role, especially for roles related to the use, management or protection of information security.
* Information security responsibilities must be communicated to employees as part of the on-boarding process.
* All employees are required to sign a Confidentiality/Non-Disclosure Agreement before being granted access to any information resource.
* Upon termination of employment, personnel must be reminded of confidentiality and non-disclosure requirements.
* (Company) will provide all employees an anonymous process for reporting violations of information security policies or procedures.

Background Checks

* Background checks are required prior to employing (Company) employees, regardless of if a competitive recruitment process is used.
* Background checks may be required for employees who change positions in the company, obtaining more sensitive duties, as determined by Human Resources or the hiring manager.
* Background checks may be required for employees at any time after the employment start date, at the discretion of Human Resources or Executive Management.
* Contractors with access to (Company) **confidential information** must have a process in place for conducting background checks on applicable staff. An agreement must be put in place specifying the responsibilities for conducting background checks if a procedure is not currently being followed or in question.

Training and Awareness

* All new personnel must complete an approved **Security Awareness** training prior to, or within 30 days of, being granted access to any (Company) **Information Resources**.
* All personnel, including third parties and contractors must be provided with relevant information security policies to allow them to properly protect (Company) **Information Resources**.
* All personnel, including third parties and contractors, must acknowledge they have received and agree to adhere to the (Company) Information Security Policies before they are granted to access to (Company) **Information Resources**.
* All personnel must complete the annual security awareness training.

Definitions

See Appendix A: Definitions

References

* ISO 27002: 7, 13
* NIST CSF: PR.AT, PR.IP, DE.CM
* Information Security Policy
* Confidentiality/Non-Disclosure Agreement

Waivers

Waivers from certain policy provisions may be sought following the (Company) Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Modified Date | Approved Date | Approved By | Reason/Comments |
| 1.0.0 | August 2020 |  | FRSecure | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |