Personnel Security Policy

Purpose

The purpose of the (District/Organization) Personnel Security Policy is to ensure adequate checks are established to determine and/or confirm, within appropriate legal and professional limits, the qualifications and suitability of a job candidate for roles within (District/Organization).

Audience

The (District/Organization) Personnel Security Policy applies to all (District/Organization) applicants and employees; full-time and part-time.

Contents

[General](#_General)

[Background Checks](#_Background_Checks)

Policy

### General

* For all roles within (District/Organization), 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.
* (District/Organization) 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 (District/Organization) employees, regardless of if a competitive recruitment process is used.
* Background checks may be required for employees who change positions in the District, 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 (District/Organization) **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.

Definitions

See Appendix A: Definitions

References

* ISO 27002: 7, 13
* NIST CSF: PR.IP, DE.CM

Waivers

Waivers from certain policy provisions may be sought following the (District/Organization) 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 | February 2018 |  | SecurityStudio | Document Origination |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |