LAST UPDATE DATE	04-24-2025
OWNER	JEFF LILLIBRIDGE
STATUS	APPROVED

PERSONNEL SECURITY POLICY

Approval History

Version	Approved By	Approved On
1.0	Not Present	04-24-2025

Purpose

To ensure that personnel security safeguards are applied to the access and use of information technology resources and data.

Scope

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

Background

Security personnel is expected to comply with a variety of methods designed to protect the companies they work for. Personnel security policy covers those methods that the organization employs to protect information systems from insider threats and malicious actors.

Policy

General

- For all roles within City of Madeira Beach, 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 during the onboarding process.
- All employees must 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.
- City of Madeira Beach will provide all employees an anonymous process for reporting violations of information security policies or procedures.

Background Checks

- Background checks are required before employing City of Madeira Beach employees, regardless of whether 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 **confidential information** must have a process 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 before 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 protect adequately (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 access to (Company) **Information Resources**.
- All personnel must complete the annual security awareness training.

Enforcement

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge and 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.