Policy Statement

Crown Castle International Corp. (Crown Castle) collects, manages, and stores information on a regular basis to support business operations. Crown Castle is committed to preserving the confidentiality, integrity, and availability of its information assets (which includes end user computing devices, servers, systems, applications, databases, cloud services, network resources, and information and data used to conduct business on behalf of Crown Castle).

Accordingly, Crown Castle shall protect its information assets, provide for the integrity of business processes and records, and comply with applicable laws and regulations.

This Information Security Policy (the "Policy"), reinforces Crown Castle leadership's commitment, establishes high-level functions and responsibilities of an information security program, and outlines the security requirements to safeguard data stored on Crown Castle's information assets. Crown Castle's Enterprise Security program involves not only the protection of data stored on Crown Castle's information assets but also includes:

- the systems and networks where data is processed, transmitted, and stored whether on premise or in the cloud,
- the physical facilities housing information assets,
- the appropriate preservation and processing of data artifacts, and
- Crown Castle users.

Authority

Crown Castle shall maintain a coordinated plan and program for information security that is implemented and maintained through policies, standards, and procedures (PSPs). Crown Castle enterprise security PSPs define the principles and terms of Crown Castle's Enterprise Security program as well as the responsibilities of Crown Castle users in carrying out and adhering to program requirements. The PSPs serve as the cornerstones by which Crown Castle data users can demonstrate that they are good stewards of the data entrusted to them.

The Crown Castle Enterprise Security program strives to ensure that enterprise security efforts consistently demonstrate a commitment to the core mission and principles of the organization while protecting the overall security of information assets at Crown Castle.

Applicability

This Policy and associated PSPs apply to all Crown Castle users (which includes teammates, customers, vendors, business partners as well as other individuals or third-parties) that are authorized to use and/or access Crown Castle information assets, associated technology, resources, and data.

Responsibility

All Crown Castle users have a responsibility to help ensure that Crown Castle's information assets are used only in the proper pursuit of the organization's mission and that the confidentiality, integrity, and availability of Crown Castle's information assets is always maintained, regardless of where the relevant data is processed or stored. All Crown Castle users have an obligation to appropriately use and protect information in a manner that is respectful of personal, customer, and corporate privacy. Crown Castle users also must use and protect information in compliance with applicable laws and regulations.

The Enterprise Security team is charged with assisting and supporting Crown Castle users in meeting these responsibilities and strengthening accountability and overseeing organizational efforts to preserve the confidentiality, integrity, and availability of Crown Castle's information assets. This includes:

- coordinating enterprise security-related activities,
- developing and implementing proactive technical and non-technical measures and controls to help detect, mitigate, remediate, and prevent security risks,
- establishing PSPs governing all facets of security, and
- providing an effective incident response when necessary.

The Director of Enterprise Security is responsible for overseeing the Enterprise Security program and team and is identified as the Crown Castle Information Security Officer (ISO).

The Crown Castle ISO is responsible for:

- Development and ongoing maintenance of this Policy,
- Compliance with this Policy and may enlist other departments in the maintaining and monitoring compliance with this Policy,
- Identifying and delegating the responsibility for enterprise security,
- Approving PSPs governing all facets of security,
- Enforcing compliance with security PSPs,
- Approving or denying exception requests for security PSPs,
- Overseeing incident response as necessary, and
- Reporting periodically to the Enterprise Security Committee (ESC), the Executive Management Team (EMT), and the Board of Directors on matters of information security.

The Crown Castle ISO is also responsible for partnering with:

- The Crown Castle **Privacy and Compliance Officers** in the development and adoption of an overall Privacy Framework,
- The Crown Castle **Internal Audit** team in the development and adoption of an overall Risk Management Framework, and

- The Crown Castle **Technology** teams, including Digital and Data, Networks and Network Operations Centers, in the development, adoption, and enforcement of PSPs.

The Enterprise Security team will maintain strong relationships with the Legal Department, Facilities, Risk Management & Safety, Digital and Data, the Business Support Department, the Internal Audit Department, and all business units handling confidential data. These partners are essential to the provision of enterprise security services and privacy protections to Crown Castle.

Compliance and Exceptions

Compliance with this Policy is mandatory and all violations of this Policy or any information security PSPs is subject to disciplinary action in accordance to applicable Crown Castle policies and standards, up to and including the termination of employment or contract, as applicable.

Requests for exceptions to any security PSPs must be submitted to the ISO. Exceptions shall generally be permitted only on receipt of written approval from the ISO or a member of the Executive Management Team after a risk assessment of the requested exception has been performed.

Governance

The Crown Castle ISO is charged with establishment of an Enterprise Security Committee (ESC) to provide input, support, and steering to the Enterprise Security program.

The ESC is a broad-based membership of senior Crown Castle leaders providing input to ensure that the implementation of security standards and policy requirements remain strong, appropriate, and in alignment with Crown Castle's mission and risk perspective.

ESC Membership and responsibilities are defined in the ESC Charter.

Communications

Crown Castle's information security PSPs are available on an Enterprise Security intranet site or other system as appropriate. The Enterprise Security team communicates to the Crown Castle organization via the Enterprise Security intranet site as well as through announcements and training, when policies or standards are created or when major revisions are published.

Reporting Requirements

Any violation or suspected violation of this Policy should be reported to a supervisor, the Enterprise Security team or by utilizing the Alert Line at 1.866.480.6138 or https://crowncastle.alertline.com.

Information security incidents (such as security breaches or loss of data) shall follow the reporting requirements outlined in the *Incident Response* standard.

Updating the Policy

The owner of this document is the ISO (or designee). It is the responsibility of the ISO (or designee) to maintain, update, and communicate the content of this document as necessary. Questions or suggestions for improvement must be submitted to the ISO.

This Information Security Policy shall be reviewed by the ISO at least annually or when significant changes necessitate a revision. Any updates to the Policy will be posted on the CONNECT Policy and Guidelines page.

Questions

Questions regarding this Policy should be directed to CyberSecurity@crowncastle.com.