Corporate Security Executive Statement

Policy Statement

It is Castle Intelligence, Inc. (“Castle”) policy objective to:

- Maintain an accessible, reliable, and secure computing environment to support its business objectives as a leading cloud-based chargeback fraud detection platform;
- Maintain integrity, availability, and confidentiality of information by protecting it from unauthorized disclosure, modification, and destruction;
- Focus protection efforts primarily on the most critical Castle resources such as proprietary software code, sensitive data, and availability of cloud and other computing resources.

Scope: this policy applies to all of Castle, Inc.

Security Leadership Committee (SLC) is the group of Castle employees and contractors that formally oversee security efforts. They may have different titles. The SLC and their formally appointed delegates are named at the bottom of this statement. Any reference to the SLC in any Castle security policy applies jointly and individually to any and all members of this group.

Security Policies include all corporate security policies and guidance documents issued to implement those policies. They may include policies, standards, procedures, guidelines, and similar documents that provide instructions or guidance to employees. In certain contexts, standards may include externally produced documents such as governmental regulations.

Responsibilities

All security related activities and responsibilities, as detailed below, must always be undertaken in a manner consistent with all applicable standards, regulations, licenses, and contracts, as well as Castle security policies.

The SLC is responsible for overseeing the enterprise security infrastructure, organization and program, updating security policies, and monitoring policy compliance. The SLC:

- Issues policies to ensure the accessibility, reliability, protection, and proper use of electronic resources available for use within Castle;
- Issues policies for protecting and classification of electronic information according to its sensitivity, criticality and value;
- Ensures that electronic resources and information are disposed of properly;
- Engages with independent auditors to validate compliance with specific rules and regulations affecting Castle business;
- Oversees security architecture, engineering, and operations across the organization;
- Establishes and implements appropriate security incident handling procedures, including security monitoring and response;
- Oversees and directs information security related activities;
- Implements an employee security awareness and training program;
- Performs an annual security policy review and updates policies as needed;
- Oversees an annual risk assessment.

Each executive or department head must:

- Ensure that electronic resources within their organization are used only by authorized personnel;
- Ensure that electronic resources and information under their control are disposed of properly;
- Ensure that electronic information is properly protected.

Each employee and authorized third party must:

- Protect Castle electronic resources and information properly;
- Act in accordance with all Castle security policies;
- Act in a truthful, ethical, and honest way while working for or representing Castle and while using Castle electronic resources.

Compliance

Castle employees who violate Castle security policies are subject to legal and/or disciplinary action, including the possibility of immediate termination. Authorized third parties who violate Castle security policies are subject to business action, including immediate loss of access, termination of contracts or other business relationships with Castle, and/or legal action. Castle will not retaliate against any individual who raises a concern regarding the Castle's compliance with this policy or who participates in an investigation related to enforcement of this policy.

Contact	Security Leadership Committee	slc@castle.io
SLC Members	Sebastian Wallin	
	Barak Engel	Rachael O'Neill
SLC Delegates		