Castle

# Cyber Security Policy

July 10, 2017

## TABLE OF CONTENTS

# I. Introduction

This Cyber Security Policy is aimed to provide an overview of Castle Intelligence, Inc., (collectively, "Castle")'s information security architecture and processes. Each subsection herein refers to the policies and procedures that may be applicable. This policy is aimed to define the security requirements for the proper and secure use of information technology resources within Castle. Castle's goal is to protect Castle and its investors and to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation and business outcomes.

Exceptions to the policies defined in any part of this document may only be authorized by the Chief Technology Officer "CTO" or the Chief Executive Officer "CEO".

All Information Technology services should be used in compliance with the technical and security requirements defined in the design of the services. Infractions in the policies in this document may lead to disciplinary actions. In some serious cases, they could even lead to prosecution.

## A. Overview

Office Location: Castle is located at 60 Rausch St #205, San Francisco, CA 94103.

The CTO is responsible for monitoring and management of Castle's network. If the CTO role is vacant, the CEO will execute duties.

Contact information for Castle's relevant cyber security and information technology service providers can be found in **Exhibit A**.

### a. Network & Connectivity Services

As Castle primarily leverages AWS for production and development work, Castle in not dependent on dedicated circuits or physical offices. Castle leverages multiple services for Internet connectivity which are secured by industry level protocols.

### b. Amazon Web Services

AWS hosts the production services of Castle. Access is highly restricted to authenticated systems and users.

## B. Computer & Storage Services

### a. Server Environment

Approximately 20 servers are hosted in AWS. Castle leverages elastic services to grow.

### b. Hosted Services

Email: Castle utilizes a hosted email solution powered by Google G Suite, where Multi-Factor Authentication (MFA) is required for all employees.

### c. Computer Equipment

Each employee maintains a laptop. Castle's CTO tracks all purchases and locations of equipment. Computers have hard drive encryption and account screen lockouts.

# II. Identification of Risks and Cyber Security Governance

## A. Documented Information Security Policy

This policy applies to desktops, laptops, printers and other equipment, to applications and software ("IT Assets"), to anyone using those assets including internal users, temporary workers and visitors, and in general to any resource and capabilities involved in the provision of Information Technology ("IT") services.

### a. Asset Policy

- IT Assets must only be used in connection with the business activities for which they are assigned and/or authorized.
- Each user is responsible for the preservation and correct use of the IT Assets they have been assigned.
- Active desktop and laptops must be secured if left unattended. Whenever possible, this policy should be automatically enforced.
- Access to IT Assets within Castle must be restricted and properly authorized, including remote access. Access to IT Assets is forbidden for non-authorized personnel.
- When traveling, portable equipment like laptops and smartphones must remain in possession of the user.
- Whenever possible, encryption and erasing technologies will be implemented in portable assets in case they are stolen.
- Losses, theft, damages, tampering or other incidents related to assets that compromise security must be reported as soon as possible to the CTO.  Disposal of assets must be done according to the specific procedures for the protection of the information. Assets storing confidential information must be provided to the CTO who will completely erase all sensitive information.

### b. Access Control Policy

- Any system that handles confidential information must be protected with a password-based access control system, at a minimum. MFA must be used for devices handling Personally Identifiable Information (PII).
- Users must refrain from trying to tamper or evade the access control in order to gain greater access than they are assigned.

### c. E-mail Policy

- All the assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of Castle. Occasional use of personal email on the Internet for personal purpose may be permitted if in doing so there is no perceptible consumption in Castle system resources and the productivity of the employee's work is not affected.

- Use of Castle resources for non-authorized advertising, external business, spam and other uses unrelated to Castle business is strictly forbidden unless prior consent is obtained from the CTO.
- In no way may the email resources be used to reveal confidential or sensitive information from Castle outside the authorized recipients for this information.
- Using the email resources of Castle for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is absolutely prohibited.
- Use of Castle email resources is maintained only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the firm, the associated account must be deactivated according to established procedures for the lifecycle of the accounts.
- Users must have private identities to access their emails and individual storage resources, except specific cases in which common usage may be deemed appropriate.
- Privacy is not guaranteed. When strongest requirements for confidentiality, authenticity and integrity appear, the use of electronically signed messages is encouraged. However, only the CTO may approve the interception and disclosure of messages.
- Identities for accessing corporate email must be protected by MFA.
- Security incidents must be reported and handled as soon as possible.  Users should not try to respond by themselves to security attacks.

### d. **Internet Policy**

- Access to Internet is permitted for all users with certain restrictions as determined by the CTO.
- The use of messenger services is permitted for business purposes, if such service is backed up and managed according to firm procedures.
- Downloading is a privilege assigned to all users. Certain sites may be blocked and unblocked at the discretion of the CTO.
- Internet access is mainly for business purpose – some limited personal navigation and use of personal messenger services is permitted if in doing so there is no perceptible consumption of Castle system resources and the productivity of the work is not affected.
- Inbound and outbound traffic must be regulated using firewalls in the perimeter. Back to back configuration is strongly recommended for firewalls.
- In accessing Internet, users must behave in a way compatible with the prestige of Castle. Attacks like denial of service, spam, phishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.
- Reasonable measures must be in place at servers, workstations and equipment for detection and prevention of attacks and abuse. They include firewalls, intrusion detection, antivirus/malware/spyware and others.

### e. **Antivirus Policy**

- All Windows computers and devices with access to Castle's network must have an antivirus client installed, with real-time protection.

- All Windows servers and Windows workstations owned by Castle or permanently in use in Castle's facilities must have an approved, centrally managed antivirus. That also includes travelling devices that regularly connects to Castle's network or that can be managed via secure channels through the Internet.
- All the installed antivirus software must automatically update their virus definitions. They must be monitored to ensure successful updating is taken place.
- Visitors computers and all computers that connect to Castle's internal network are required to stay "healthy", i.e. with a valid, updated antivirus installed.

### f. **Remote Access Policy**

- To gain access to the internal resources from remote locations, users must have the required authorization. Remote access for an employee, external user or partner can be granted only by the CEO.
- Only secure channels with mutual authentication between server and clients must be available for remote access. Both server and clients must receive mutually trusted certificates or public key cryptography.
- Remote access to confidential information should not be allowed, unless such access is strictly needed.
- Users must not connect from public computers unless the access is for viewing public content.
- Everything is either on drive or AWS, secured by MFA. Encrypted Flash drives are used for production system key storage.

### g. **Outsourcing Policy**

- Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications.
- In any case, the service provider should be selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties.
- Audits should be planned in advance to evaluate the performance of the service provider before and during the provision of the outsourced service, function or process. If Castle has not enough knowledge and resources, a specialized company should be hired to do the auditing.
- A service contract and defined service levels must be agreed between Castle and the service provider.
- The service provider must get authorization from Castle if it intends to hire a third party to support the outsourced service, function or process.

### h. **Data Destruction Policy**

- Any computer system, electronic device or electronic media is disposed, recycled or transferred either as surplus property or to another user, the system, media or device must be either:
    - Properly sanitized of sensitive/confidential data and software, and/or
    - Properly destroyed or donated.

- Any print, facsimile or other physical media.

### B. Periodic Assessment of Cyber Security Risks

Castle’s security team periodically assesses cyber security risks to the firm.

### C. Periodic Assessment of Physical Security Risks

Each employee keeps a list of all hardware devices and regularly reviews this list to ensure that all hardware is accounted for.

### D. Cyber Security Roles and Responsibilities

Castle’s CEO with the assistance of the CTO, is responsible for the oversight of Castle’s Cyber Security Policy.

### E. Business Continuity Plan

Castle maintains a Disaster Recovery/Business Continuity Guide, also attached hereto as **Exhibit A**. Castle's disaster recovery plan is designed to provide Castle employees with secure and seamless access to mission critical network systems using their laptops/desktop computers from any location in the world with a connection to the Internet.  Planning for disasters includes real-time replication, monitoring and daily backup of mission critical network systems at remote locations. Certain “Critical Users” are given priority when restoring access.

## III. Protection of Firm Networks and Information

### A. Cyber Security Risk Management Standards

Castle does not at present use a formal cyber security risk management standard such as ISO or NIST. However, Castle has adopted a cyber security risk management program which implements a number of procedures and controls that significantly reduce cyber security risks to the firm.

#### a. Employee Training and Written Guidance

Castle provides biannual compliance training to its employees which will provide an overview of Castle’s information security policies and procedures. This Cyber Security Policy serves as the employees’ written guidance concerning information security risks and responsibilities.

#### b. User Privileges and Network Access Control (NAC)

Castle’s CTO is responsible for maintaining network access and authentication. Network accounts must be implemented by the CTO and may be configured to request authentication at startup.

#### c. Protection Against DDOS Attacks

Castle relies on AWS mechanisms to protect against DDOS.

### d. Documented Cyber Security Incident Response Plan

If a security incident or breach of any cyber security policy is suspected, Castle employees must immediately notify security@castle.io, including as much information as possible as to what happened and the potential scope of the incident.

Such incidents may include suspected compromise of login credentials, suspected malware/virus, or the loss of any device containing Castle information.

## B. Use of Encryption

No highly confidential data is stored. Passwords are salted and hashed.

Stripe is leveraged for credit card data.

TLS is leveraged for data transmission. All laptop hard drives are encrypted. Periodic Compliance Audits of Security Policies

Castle's CTO regularly reviews Castle's internal cyber security policy to ensure it is up-to-date. Castle may conduct periodic audits of employees' devices.

## C. Cyber Security Assessment of Third Parties

Castle evaluates its third party service providers if it determines a cyber security risk is posed by nature of the third party's relationship with Castle. In particular, Castle categorizes its third party service providers into three categories ("High," "Medium," and "Low" sensitivity levels) based on the third party's access to the firm's data and reputational risk. For third parties with access to nonpublic personal information concerning investors, they are automatically categorized as "High" sensitivity level. Based on the documentation provided by the third party in response to Castle's requests, Castle then ranks the third parties' responses as "Strong," "Moderate," or "Weak." The following actions will be taken depending on the rankings:

- Strong: Third parties with a "Strong" rating will be reevaluated on an annual basis.
- Moderate: Third parties with a "Moderate" rating will be reevaluated in six months after Castle aims to identify areas for improvement in the third parties' policies.
- Weak: Third parties with a "Weak" rating will be reevaluated immediately. Castle will aim to identify the primary gaps in the third parties' information security policies and procedures and will ask for evidence of the third party's attempts to address its concerns.

## D. Cyber Security Training Materials for Third Party Vendors

Castle does not utilize cyber security training materials for third party vendors at this time. However, the CTO in their discretion, may require third party vendors to provide documentation of internal cyber security and information technology policies.

### E. Network Segregation of Third Party Access/Content

Castle segregates as best possible its infrastructure and resources from third parties. When it is necessary to grant access to a third party, the access is restricted and carefully controlled. Any request for third party access must be approved and implemented by the CTO and CEO.

### F. Logging and Control of Third Party Network Access

Third parties are provided only the minimum access necessary to perform the function requiring access. When possible, systems requiring third party access are placed in a public network segment or demilitarized zone (DMZ) in order to protect the internal network.

## IV. Detection of Unauthorized Activity

### A. Baseline of Network Traffic and Events

Castle analyzes network traffic and provides forensic-level monitoring for unusual network behavior and other indicators of compromise therein. Amazon CloudTrail is leveraged to monitor AWS access.

### B. Event Aggregation and Correlation

Castle performs forensic-level analysis and alerting when appropriate.

### C. Detection of Cyber Security Events/Intrusions

Castle utilizes software which can analyze network traffic and provides forensic-level monitoring for unusual network behavior and other indicators of compromise therein.

### D. Detection of Malicious Code on Network/Mobile Devices

Castle can analyze network traffic and implement forensic-level monitoring for unusual network behavior and other indicators of compromise therein.

Castle regularly performs scanning for vulnerable software and systems within the environment.

### E. Monitoring Third Party Activity

Castle monitors the remote access by third party service providers internally.

### F. Detection of Unauthorized Users, Devices, Software

Castle regularly monitors for the presences of unauthorized connections and software within the firm’s networks.

### G. Penetration Testing and Vulnerability Scanning

Castle performs vulnerability scanning from multiple perspectives (external, internal, network traffic), and as noted above, performs scanning for vulnerable software and systems within the environment.

Every calendar year a third party executes a penetration test on Castle’s production infrastructure.

# V. **Other Cyber Security Information**

## A. **Cyber Security Incidents**

### a. **Malware Detections**

Castle continuously monitors its network for breaches and reviews denial of service attacks and helps identify what resources were affected and the method of the attack. Any material attacks are documented.

## B. **Reporting a Cyber Security Incident**

If a cyber security incident is suspected, Castle employees must immediately notify security@castle.io as necessary, who may report the incident to the following entities:

- Law enforcement
- A state or federal regulatory agency
- An industry or public-private organization facilitating the exchange of information about cyber security incidents and risks.

## C. **Cyber Security Budget**

Castle will review on an annual basis whether its annual budget for cyber security, privacy and IT security programs is sufficient given the size, potential risk to the firm and resources of the firm.

# Exhibit A. **Disaster Recovery and Business Continuity Plan**

## Business

Castle Intelligence, Inc. (“Company”) has developed this Disaster Recovery and Business Continuity Plan (“Plan”), in collaboration with Stealth Worker, Inc., to address all manner of threats to the continuity of business operations.

## Key Personnel

For each key personnel, we have identified the accounts that they hold credentials to. These are shared securely with the rest of the team to enable business operations to continue even if key personnel become unavailable. Contact and emergency contact information are stored securely. SSH access to production servers is only available for key personnel via a secure VPN connection.

## Non-key Personnel

The data and work products of all non-key personnel are accessible via internal company systems, including:

- GitHub storage of all checked in application code
- Google Drive storage of all application documentation
- Amazon Web Services (AWS) Web Console access to development environment settings

## Physical Locations

Physical locations are subject to disruption through fire, flood, earthquake, hurricane, utility or power outage, war and civil disorder. Company minimizes these threats through the use of third parties for hosting of application development and production servers.

- Multi-availability zones in the USA currently
- Full multi-region will be completed in Q2 2017

Set of admins: 3 admins have access to each core system, so in the loss of one key team member, nothing is lost.

## Server Operations and Disaster Recovery

Castle exclusively uses AWS for hosting of staging (development environment) and production servers. Our system is configured to operate in multiple availability zones to create robustness against individual AWS data center outages.

## Response to Epidemic

During an epidemic outbreak, Company will group staff into separate teams, and rotate the teams between primary and secondary work sites and/or require remote work, with a rotation frequency equal to the incubation period of the disease. During an epidemic, Company will ban face-to-face intergroup contact during business and non-business hours. The split increases resiliency against the threat of quarantine measures if one person in a team is exposed to the epidemic.

## Response to Cyber Attack

This is covered in the Incident Response Plan.

## Response to Theft

Company physical data storage is limited to AWS servers, Company-owned computers, and Contractor-owned computers. Computers are not stored at company offices.

## Response to Random Failure of Mission Critical Systems

We have architectured the AWS infrastructure to ensure there is no single point of failure. Disaster recovery is built in both in each site and between multiple sites.

## Business Continuity Plan Maintenance

The CEO is responsible to make sure the Plan is periodically reviewed and updated to support the Company's operations, growth, legal obligations and personnel safety. The Plan shall be reviewed not less than annually.

## Revision History

- Document updated July 10, 2017
- Document created July 30, 2016