Security Administration Manual

Policy Statement

Successful administration and operations of security tasks is a key element in managing data security at Castle. This document centralizes and organizes these policies, guidelines, standards and procedures.

Scope: This policy applies to all Castle employees and third parties managing or otherwise participating in the administration of Castle's production system security operations, and is part of the Castle corporate information security policy.

Security Operations

Responsibility: Security operations are the direct responsibility of the Security Leadership Committee, who may further delegate such responsibility. For purposes of this policy, the security team has been formally delegated security operations responsibilities within Castle's service delivery (production) infrastructure.

Outsourcing to Third Parties: Castle security operations tasks can be outsourced to third party vendors, as long as the company's Security Leadership Committee authorizes this decision.

Compliance: Castle security operations tasks are required to satisfy all relevant requirements from any laws, rules and regulations that might have an impact on company operations (PCI, HIPAA, GDPR, etc). Under no circumstances is it permissible to remove or change the scope of security operations tasks without a security department review of the proposed impact of such a change.

Awareness: All employees must be made aware of security as it pertains to their role. To achieve that goal, the security awareness program will employ multiple mechanisms, such as emails, automated awareness and education systems, annual acknowledgments of policy, targeted education such as secure coding training for developers, meetings and so on.

Ongoing/Daily/Weekly Tasks

1. Examine reports from intrusion detection, file integrity, cloud and system security event logs
2. Manage daily change control as necessary
3. Manage security incidents as necessary
4. Identify and recommend critical security patches issued by vendors, if any
5. Read new advisories issued on major advisory lists (e.g. Bugtraq)
6. Issue relevant internal and external security advisories and announcements
7. Update security baselines such as file integrity databases (at least weekly)

Monthly/Quarterly/Semi-Annual Tasks

1. Using a risk-based approach, discuss vendor-released patches and discovered vulnerabilities.
   a) Validate, and correct if necessary, security patch deployment across the entire environment so that no critical or high (CVSS > 7.0) security patches are outstanding for more than 30 days and medium (CVSS > 4.0) for more than 90 days, unless an internal risk evaluation determines that such patches can be deployed beyond this time frame.

2. Perform external vulnerability scans against the cloud production platform (quarterly)
3. Audit production user accounts, disable/remove accounts idle for more than 90 days (quarterly)
4. Review and ensure that network diagrams are current and reflect the actual network environment (quarterly, and after any major network change)
5. Perform review of firewall and security group rules across the entire production platform (semi-annually); this task can be performed continuously instead, as long as an audit trail (e.g. via tickets, emails, or similar logs) exists of such review

Annual/Bi-Annual Tasks

1. Perform annual network and application penetration tests by a third party
2. Perform annual PCI audit by a qualified assessor
3. Test security controls for effectiveness
   a) examine the Security Testing Guideline (in this document) for further detail
4. Perform a security policy review; this task may be performed continually, as reflected by advancing policy version numbers and publication dates
5. Obtain security policy acknowledgments from all employees
6. Perform a security risk assessment (at least for PCI data)

Services Overview

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.

Amazon Web Services: AWS hosts the production services of Castle. Access is highly restricted to authenticated systems and users. Amazon CloudTrail is leveraged to monitor AWS access

Computer & Storage Services:
Hosted Services: Castle utilizes a hosted email solution powered by Google G Suite, where Multi-Factor Authentication (MFA) is required for all employees.
Server Environment: Approximately 20 servers are hosted in AWS. Castle leverages elastic services to grow.

Financial Services & Budget:
Client Financial Services: Stripe is leveraged for credit card data
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.

Asset Management Overview

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

Global Operations Requirements

System Hardening: Castle must ensure that all devices handling sensitive data in its environment are properly configured (hardened) in a secure manner. Configurations must protect against known vulnerabilities and based on established best practices, such as implementing a single primary function per server. To this end, Castle will rely on tools such as the Center for Information Security (CIS)'s benchmarking utility available to CIS members.

NTP: All production systems must have the time service (NTP) installed, operational, and utilizing an industry accepted time source, and wherever possible in order to avoid drift, doing so via centralized systems within the Castle production environment which peer with each other. This requirement will typically be addressed via built-in mechanisms in AWS.

Vulnerability Scanning

Castle operates in a cloud environment, running on the Amazon cloud. This creates some limitations on Castles ability to perform scanning against its virtual machines in the Amazon cloud, since Castle does not control the network layer. Within the AWS environment; there is no concept of an “internal network” beyond what is available to an administrator that has already successfully accessed the service environment, and such a distinction is not made for the purposes of scanning.

Scans: in the context of this environment, Castle performs recurring externally-originated (cloud-based) authenticated scans against its platform in AWS. Such scans are also performing following any significant changes to the environment. Scan reports must be maintained for at least 12 running months.

Firewall Administration

Firewalls, whether physical or virtual, are a practical necessity and a first line of defense against network based attacks and intrusions. In addition, firewalls are required in order to satisfy rules and regulations affecting Castle's business and the business of its customers.

Intrusion Detection/Prevention Systems (IDS/IPS), whether physical or virtual, are a practical necessity as well, providing important feedback about attempted intrusions and supporting the ability to respond quickly to a mounting attack. IDS/IPS are also required in order to satisfy rules and regulations affecting Castle’s business and the business of its customers.

This policy applies to all Castle firewalls and packet filtering devices that are network-based (see below), and the personnel managing them. It does not apply to personal firewalls installed on computers.

The term “firewall”, as used in this document, generally applies to IDS/IPS as well.

Firewall: a security system that controls and restricts both network connectivity and network services. Firewalls establish a choke point where access controls are enforced. Connectivity reflects which systems can exchange information. A service or application refers to the way for information to flow through a firewall. Examples of services include FTP (file transfer protocol) and web browsing.

Firewall, Other (firewalling device): A device may sometimes act as a firewall even though their primary function is not that of a firewall. For example, a router may serve a secondary firewall function by using access lists. All Castle devices acting in the role of a network-based firewall, whether called firewall or not, must be managed according to this policy. AWS security groups fall under this category.

Application Firewalls: A security system that functions as a firewall for a particular protocol or service (e.g. WAF – Web Application Firewall). Application firewalls are considered a firewall as well.

Administration/Management

Firewall Administrator: An employee whose job function requires that they manage or configure firewalls. Castle operates inside of the Amazon AWS cloud, which means that its firewall administrators do not have access to manage the devices themselves, and instead can only manage firewall rules via the AWS abstraction layer called security groups. Office (physical) firewalls are managed by IT.

Defined Decision Maker: Before being enabled, all new rules must be evaluated for business needs and security risks. For AWS security groups, Infrastructure team members are the only decision makers recognized by policy that can approve or deny these requests, but they may formally delegate this responsibility to other employees within the organization. Security Leadership Committee are the decision makers for all other firewalls.

Firewall Change Control: Firewalls are considered to be production systems. Thus, changes to firewall rules must never be implemented without going through Castle’s change control process.

Administration/Technical

Access Privileges: Privilege to modify the configuration of any Castle firewall is restricted. Unless permission from the Security Leadership Committee or their delegates has been obtained, such privileges must only be granted to full-time employees of Castle with a role specifically requiring such privilege (i.e. firewall administrators).

Default Denial: Every service and connectivity path not specifically permitted by this policy (and any supporting documents issued by the security department) must be blocked by default.

External Connections: All incoming real-time connections to Castle's cloud environment must first pass through a perimeter firewall.

Change Logs: All changes to firewall rules must be logged, for example via a change control ticket. These logs must be kept for a period of at least 1 year.

IP Masquerading (NAT): Where practical (such as in VPC's), firewalls must be configured to "hide" internal IP addresses by utilizing NAT.

IP Filtering Baseline: All edge firewalls in the Castle environment and under Castle control must be configured to (1) disallow incoming packets with a "private" source IP address (as defined in RFC1918), and (2) disallow incoming packets with a local source IP ("spoofed packets").

2-factor/channel Authentication (MFA/2FA): In order to minimize the risk of unauthorized disclosure of information or access, all remote administrative connections to the Castle Amazon environment must be authenticated using two distinct factors (e.g. tokens) or channels (e.g. GAuth).

Configuration Auditing: due to the critical nature of firewalls in protecting against unauthorized access, all Castle's firewall rules must be audited on a regular basis, either continuously or at least semi-annually.

Permitted Services: the list of currently pre-approved services and connectivity paths must be documented and distributed to all firewall and system administrators with a legitimate need-to-know. The services listed below are the only ones pre-approved in order to support Castle's business objectives. Note that while the services listed below are considered appropriate, they may not be necessary.

- **Internal Paths**: Castle utilizes many management and security tools requiring specific service ports, such as Chef and Sensu. These ports are considered approved and are configured between different Amazon groups as necessary.
- **Incoming Traffic:** Castle limits incoming traffic to the following ports by default: (1) SSH (22) for remote access to the bastion host; (2) ports 80/443 for HTTP/HTTPS access through AWS ELBs.
- **Outgoing Traffic:** Castle does not limit outbound traffic, since as part of the service, customers may configure the platform to interact with any other publicly available system.

Justification and Documentation: Every firewall rule not explicitly included in this guideline must have a documented business justification. Such documentation may take the form of textual notation explaining the rule within the respective firewall ruleset, a ticket in the ticketing system, an email trail, a separate guideline, and so on. New rules must be approved by the Infrastructure department.

Passwords Distribution Guideline

When distributing passwords, care must be taken to ensure that passwords are not disclosed to any party other than the intended recipient. Therefore, the best method for distributing passwords is through a personal, face-to-face exchange between the password administrator and the user.

Sensitive data (e.g. private encryption key-blocks) cannot be communicated directly using this guideline. Such data must be protected (e.g. via a password-protected zip file), the password communicated via an approved method, and then utilized to access the data.

In instances where this approach cannot be used, the following guidelines apply:

- Passwords may be communicated via phone, as long as both parties ascertain that there is no risk of accidental disclosure through a third party overhearing the conversation
- Passwords may be communicated via encrypted chat or VoIP. Care must be taken to use a chat or VoIP tool that supports strong encryption. Skype and similar tools offer this option, but it must be verified to be turned on before the exchange of messages. Slack is not an acceptable platform for exchanging passwords or other sensitive data.
- If necessary, end-user passwords, or passwords used to access non-sensitive resources using non-privileged access, may be communicated using an out-of-band method. For example, the user ID may be communicated in email and the password subsequently sent via text message (SMS), as long as neither message provides an obvious link to the other.

Security Testing

Castles operational environment may contain sensitive information, such as PII. This poses a potentially significant risk to the company. In addition, standards and regulations such as HIPAA, PCI, and CIPA all mandate a rigorous security approach to protecting such information. In order to address these risks and business requirements, Castle has developed a policy of regular security testing of operational systems.

Baseline: Only the Security Leadership Committee, their appointed delegates, or third parties contracted by the team for the purpose of performing security testing services are allowed to do so within Castle’s environment.

Security testing is defined as any type of activity that aims to discover information about a device or network (reconnaissance), identify vulnerabilities, manipulate a device in an unauthorized manner, break into or hack a device, etc. For example, network mapping, penetration testing, vulnerability scanning, password cracking and attempts to test the security knowledge of coworkers all fall within this category. Activities designed to collect information for prohibited investigative purposes are similarly included.

Testing Guidelines

Random testing: unscheduled non-intrusive testing may be performed at any time by the Engineering team. Intrusive testing (any test that might somehow alter the function or performance of a target machine) must be coordinated with relevant information and system owners in advance.

Regular vulnerability scans: see vulnerability scanning at the top of this document.

Penetration tests: Castle must arrange to perform third party annual penetration tests of the company’s cloud service delivery environment. Reports of these tests must be kept for at least 2 years from the date of the test, and will be made available to auditors and similar entities as required. Additional penetration tests are to be performed in the event of a significant architectural change to the cloud environment.

Application tests: application code must be tested regularly for security issues. For more information, refer to the Software Development Life Cycle (SDLC).

Use of and Access to Customer Data - employees are prohibited from using live customer data in testing, unless with the explicit knowledge and consent of the customer. Under no circumstances are employees permitted to store customer data on local storage devices without management approval.

Wireless Networks

Wireless networks (including WiFi, Cellular and similar technologies) are ubiquitous in corporate environments, supporting increased productivity for many employees, contractors and vendors. However, wireless networks also pose a greater risk to corporate networks than wired networks, and therefore must be deployed with added caution.

The Amazon cloud environment does not allow or support wireless access. The following guideline therefore applies to the corporate environment and satellite offices.

Acceptable Wireless Implementation

Following are acceptable wireless implementation rules. Note that wireless networks may be configured in different fashions, but any deviation from the rules below must not increase risk for the environment. Generally, all such deviations should be approved in advance by a member of the security team.

Wireless Encryption: wireless networks must be configured to use a proven modern wireless encryption algorithm, such as WPA2. WEP is not allowed, except for guest WLANs as defined below.

Guest WLANs: “guest” wireless LANs must only provide access to the public Internet, and not to internal networks. Guest wireless networks must require a password with a minimum of 9 characters. It is recommended that this password be rotated at least annually.

Anti Virus Administration

To minimize the risk that viruses and other malware harm the Castle network, anti-virus solutions must be deployed on commonly vulnerable systems. Generally, every computing device except those listed below must incorporate an active, updated anti-virus solution.

Castle mandates the use of centralized anti-virus management systems to enforce all anti-virus and anti-malware requirements. The centralized AV management platform must maintain AV logs for all managed systems for a period of at least 1 year.

Recognizing that the biggest virus threat comes from unprotected computers running a Windows operating system, the following clarifications are made:

- Macs are not exempt from anti-virus requirements.
- Computers running a Sun/Solaris, *NIX or LINUX-based operating system are exempt from anti-virus requirements.
- New computers undergoing installation may be connected to the network for the purpose of downloading and installing an anti-virus solution; this step must be performed before installation of any other software.
- Devices other than computers (laptops, desktops) – for example, smartphones – are exempt from the anti-virus requirements unless they run a Windows-based operating system.

Encryption

Encryption Key Custodians: all members of the Castle team who, as part of their work duties, must interact with encryption keys in generation, rotation, and revocation processes are considered key custodians, and must fill the Castle Key Custodian Acknowledgment Form.

Key Management Requirements

Strong Keys: encryption keys must be of sufficient strength to resist brute-force attack based on current technology. For guidance, refer to the NIST 800-57 special publication, summarized here: http://www.keylength.com/ (click on the most recent NIST recommendations)

Secure Distribution: keys must be distributed in a secure fashion. Ideally, distribution should not occur at all, but rather all operations should occur in a centralized, secured location, and ideally, a feature of the cloud platform.

Secure Storage: keys must be stored securely and protected from unauthorized access.

Key Rotation and Substitution: keys must be rotated according upon cryptoperiod expiration based on the types of keys used. For guidance, refer to the NIST 800-57 publication as per Strong keys, above. Keys must however always be protected against substitution by unauthorized personnel.

Mandatory Replacement: keys must be replaced if known or suspected as weakened or compromised, or when key custodians with knowledge of clear-text keys leave the organization.

Split Control: in cases where manual, clear-text key operations are in use, no single key custodian may possess the entirety of any encryption key in use.

Remote Access Administration

Remote Access VPN: creation and deletion of VPN accounts that provide remote access to the production environment is closely controlled, and is only performed by members of the Infrastructure team. New access should only be granted with the approval of engineering leadership. All accounts must have a key pair installed to supplement password authentication.