Network and Access Control Policy

Policy Statement

Accessing and utilizing electronic resources creates risks associated with the methodologies used for such access. This policy establishes management direction, procedures and requirements for network and access control to ensure the proper protection of Castle electronic information.

Scope: This policy applies to all Castle employees, contractors and third parties (“users”) using its electronic resources, and is part of the Castle corporate information security policy.

General Controls

Mandatory Authentication: All users wishing to establish a connection with Castle systems must authenticate themselves before gaining access.

Anti-Virus: Devices must employ an anti-virus solution where applicable, as described in Appendix II, *Anti Virus*, at the end of this policy.

Testing Security Controls: Users must not test or attempt to compromise system security measures unless specifically approved in advance by the CISO. Incidents involving unapproved hacking, password cracking, use or illegal copying of software, or similar unauthorized attempts to compromise security measures may be unlawful, and will be considered serious violations of policy. Customer requests that Castle security mechanisms be compromised must not be satisfied unless: (a) the CISO pre-approves them; or (b) Castle is compelled to comply by law. Short-cuts bypassing security measures, as well as pranks and practical jokes involving the compromise of security measures are prohibited.

Compliance: All users wishing to use Castle systems must sign a compliance statement prior to getting a company user ID, and on an annual basis thereafter, indicating their understanding and agreement to abide by Castle security policies and procedures, including the instructions contained in this document.

Applicability: Unless explicitly stated otherwise, the controls listed in the remainder of this policy are only mandated for accounts with access to service delivery environments (e.g. AWS) and source-code repositories (e.g. GitHub). It is recommended that similar controls are applied elsewhere as well, and may be mandated on a case-by-case basis depending on the nature of related access (e.g. for backoffice cloud-based accounting systems). Test accounts that contain fake data used solely for testing purposes are generally exempted from these requirements.

Security Parameters: Financial account numbers, login passwords, and other parameters that can be used to gain access to goods or services, must not be sent over the Internet in readable form (such as via email), and must be encrypted in transit using a current, secure protocol (e.g. TLS 1.2+).

User Passwords

Passwords are a common access control mechanism. Passwords in use at Castle must adhere to the standard defined in Appendix I, *Password Standard*, at the end of this policy.

Password Storage: Passwords must not be stored in readable form in batch files, login scripts, or in other locations where unauthorized persons might discover them (such as written down on a sticky note attached to the bottom of a keyboard). Administrators must configure systems to store passwords in hashed and salted (rather than encrypted) form, so that they are not recoverable.

Unwarranted Disclosure: Aside from initial password assignment and password resets, if there is reason to believe that a password has been disclosed to someone other than the authorized user, the password in question must be immediately changed.

Password Distribution: Generally speaking, user passwords should not be communicated in email, using an alternative method instead (phone, encrypted chat, text, etc).

First-time Passwords: Initial user passwords must have a randomized initial value and be valid only for the new user's first connection. At that time, the user must be forced to choose another password. This same process applies to the resetting of passwords in the event that a user forgets a password.

Sharing Passwords: Passwords (except first-time ones) must never be shared or revealed to anyone else besides the authorized user.

Authentication System

All devices connected to Castle networks must have automated access controls. Servers must employ individual, unique user-IDs and passwords, as well as role-based privilege restriction mechanisms. End-user systems (e.g. laptops) must enforce a login password and include a screen saver.

Masking: The display and printing of access passwords must be obscured such that unauthorized parties will not be able to observe or subsequently recover them.

Vendor Default Accounts: All vendor-supplied default account should be disabled wherever possible, and their passwords must be changed before use in Castle.

Compromise – Forced Rotation: Whenever system security is compromised, or even if there is a convincing reason to believe that it has been compromised, the involved system owner or administrator must immediately: (a) rotate all relevant passwords, and (b) force every password on the involved system to be changed at the time of the next log-in, preferably via programmatic means, or alternatively by sending a broadcast message to all users telling them to change their passwords.

Shared (Group) Accounts: Access control must be achieved via individual, unique accounts, or otherwise include logging mechanisms that can provide an audit trail tying each action taken to the user taking it. Access to system resources via shared, group accounts is generally prohibited.

Login/Logout: All users must be positively and uniquely identified prior to being able to use any server or communications system resources.

Idle Timer: If there has been no activity on an Castle server or remote access device (e.g. VPN) for 15 minutes, the system in question must automatically suspend the session and blank the screen. The session must only be re-established after the user has re-authenticated.

Anonymous Login: Castle users are prohibited from logging into any Castle system or networked resource anonymously (e.g. by using a "guest" account). If users can change roles while being logged in to gain additional privileges, they must initially login with their own user ID before changing roles (such as via “sudo”). Direct “root” (UNIX/LINUX) or “admin” (Windows) remote logins are prohibited. Logs must record all changes of current user IDs, and track all administrative actions taken individually by each user.

System Privileges

Limiting System Access: The access privileges of all users, systems, and automated software agents must be restricted based on the principle of need-to-know. Access rights must therefore not be extended unless a legitimate business need for such access rights exists.

Non-Employees: Individuals who are not Castle employees must not be granted a user ID or otherwise be given Castle access privileges without advance written management approval.

Screen Savers: Users with Macs, PCs, Laptops and similar devices are responsible for administering a screen saver (with a timeout of 15 minutes, as per *Idle Timer* above).

Privilege Assignments: Requests for new user IDs and new or modified privileges must be tracked and approved by the user's manager. To help establish accountability, audit trails (paper or electronic) reflecting these requests must be retained for a period that extends for at least 6 months following termination of employment or contract that required such access.

Special Privileges: Administrative system privileges must be restricted to those directly responsible for systems administration or security. An exception can be made only with CISO approval.

Vendor Access: Third party vendors must not be given remote access (e.g. VPN) privileges to Castle systems or networks without explicit and legitimate business need. Such access must be enabled only for the time period required to accomplish the approved tasks (e.g remote maintenance), require 2-factor authentication, and be authorized by the CISO.

Termination Notices: Management must promptly report all significant changes in duties or employment status to the system administrators responsible for user IDs associated with the involved persons. All access for terminated employees must be removed no later than 7 days following termination.

Changes

Making Changes: With the exception of emergency situations, all changes to Castle systems and networks must follow the Castle change management and control processes. Emergency changes must be made only by authorized personnel.

Audit Trails: All security event logs must be turned on, and available online for at least 1 year.

End User Devices and Technologies

End user computing devices (e.g. smart phones, USB keys, laptops) may only be used by authorized personnel in an approved manner. Note, in particular, that connecting such devices to the production environment is prohibited unless specifically needed for performing necessary administration tasks.

All laptops in use by Castle personnel whose job duties require them to administer production systems must have a personal firewall running and active at all times.

Appendix I – Password Standard

Poor password controls present a big risk in a connected environment, potentially allowing unauthorized access that is difficult to detect and prevent. Thus, administrators and users must follow this standard in choosing their access passwords. In most cases, the system will enforce this standard automatically.

Password Composition

At a minimum, an acceptable password is “long and complex”, which is defined as a password that (a) utilizes at least 3 of the 4 categories of characters listed below, and (b) is at least 9 characters long. Example: “APassw0rd” (9 characters, small and capital letters, and a number).

CAPITAL letters	small letters	Numbers (0-9)	Special characters

However, it is strongly recommended that users employ a **passphrase** instead. A passphrase is defined as a password that (a) includes multiple distinct words or character blocks, (b) utilizes at least 3 of the 4 categories of characters listed below, and (c) is at least 12 characters long. Example: “This Password” (one space, two words, small and capital letters). Passphrases are much easier to remember, and can be thought of as natural language phrases.

Administrative Password Controls (system-enforced)

Rotation: Passwords to administrator accounts, or to production service environments, or those that provide access to storage systems with sensitive information, must be rotated every 90 days. Other user passwords may be rotated annually, as long as access also incorporates 2-factor/2-channel (e.g. google-auth) authentication.

Reuse: when rotating their password, users must not reuse any of their last 4 passwords.

Lockout: User accounts for Castle’s production environment must be locked out after 6 failed consecutive login attempts. This lockout may be removed manually by an administrator, or automatically by the system after 30 minutes.

Specific Exceptions

The following exceptions are specifically allowed:

Customer Passwords: passwords for Castle's customers are generally exempt from password standards, although it is recommended that they be at least 8 characters long.

Service Account Passwords (SAPs): accounts utilized for automated (software or agent) access from Castle systems to other Castle systems must utilize a complex, random, long password, ideally generated by a random password generation tool while allowing “lookalike” characters. Such passwords must be at least 16 characters long. SAPs must be (a) rotated annually; (b) using a newly generated random value; and (c) locked-out after a single failed login attempts, with an alert generated by an administrator for manual handling only. Each application must have its own, assigned SAP.

Appendix II – Anti-Virus

Viruses, trojans, worms and other forms of malware have become prevalent as part of a connected world, and present significant risks to computing resources. To address this risk, a Windows or Mac PC connected to Castle's network, must:

- Include an anti-virus (AV) solution that has been approved by the company's IT department
- Include protections against spyware, adware and other forms of malware
- Have the most recent signature file available installed
- Have the AV solution active, scanning all incoming connections, files, and emails.

The IT department will immediately disconnect and shut down computers in violation of this policy, until a proper solution is installed on the computer and it has been cleaned.

In order to minimize the chances of a virus infection:

- Always run AV software supplied by or approved by the IT department. When in doubt about AV software, submit an email request to the IT department.
- Always configure AV software to automatically download and install new signatures at least daily.
- Never download or open any files from unknown or suspicious sources.
    - Always delete and purge such files and/or the messages containing them. If you are unsure as to the safety of opening any file, it is best to leave it unopened.
    - If possible, it is always best to download files that have been digitally signed by a trusted source, and to verify the digital signature before opening the file.
- Avoid network or file sharing unless there is a business requirement to do so.
- Always perform an AV "full-scan" on new media (such as DVDs or USB drives) received from unknown sources.

If you suspect that your computer has been infected by a virus, immediately contact the IT department.