Acceptable Use Policy

Policy Statement

The wide array of resources, services, and interconnectivity available via the Internet all introduce risks. In response to these risks, this policy describes Castle's policy regarding Internet use and security.

Scope: this policy applies to all Castle employees and third parties using Castle's electronic communications and data infrastructure.

Information Integrity and Confidentiality

Information Reliability: A considerable amount of information found online is outdated and inaccurate, and sometimes deliberately misleading. Accordingly, employees should use care before relying on such information for business decision-making purposes.

Information Exchange: Castle internal information must not be transferred to third parties for any reason other than expressly authorized business purposes. Exchanges of such information with any third party may not proceed without an NDA in place.

Disclosing Internal Information: Employees must not post Castle internal information online unless such a posting has first been approved by Castle management, since such disclosures may adversely affect Castle's business, valuation, customer relations, or public image. Examples include business prospects, products in R&D, release dates, internal systems problems, and so on. Information that is intended to be shared, such as appropriate responses to customer support requests or scheduled outage notices, are exempted from this policy.

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, and must be properly encrypted in transit (e.g. TLS 1.2+).

Public Representation

No Misrepresentation: Except where anonymity is expected (e.g. web browsing), misrepresenting, obscuring, suppressing, or replacing a Castle user's identity online is forbidden. The employee's name, email, organizational affiliation, and related information included with online postings must reflect the actual poster.

External Representations: Employees may indicate their affiliation with Castle in forums, social networking sites, chat sessions, etc. This may be done by explicitly adding certain words, or it may be implied, such as via a Castle email address. Whenever employees provide such an affiliation when not handling work duties, they must also clearly indicate the opinions expressed are their own, and not those of Castle. Likewise, if an affiliation with Castle is provided, political advocacy statements and product or service endorsements are also prohibited unless they have been previously cleared by Castle management. With the exception of ordinary marketing and customer service activities, all representations on behalf of the Castle must first be similarly cleared by Castle management.

Online Business Representation: Employees may not establish new online presence, or make modifications to existing online presence, dealing with Castle business, unless they have first obtained the approval of their department head. This will ensure that all posted material has a consistent and

polished appearance, is aligned with business goals, and is protected with adequate security measures. Castle employees whose jobs requires them to modify Castle online properties are allowed to do so without prior approval, as long as the changes are (1) authorized as part of their regular job duties, (2) do not harm the appearance, performance or reliability of the relevant online property; and (3) do not harm the confidentiality, integrity or availability of the information contained in the relevant online property.

Appropriate Behavior: To avoid libel, defamation of character, and other legal problems, whenever any affiliation with Castle is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited. Likewise, employees must not make threats against another user or organization, online or otherwise. Internet messages intended to harass, annoy, or alarm another person are similarly prohibited. Please see the ***Social Networking*** appendix for further guidance.

Removal of Postings: Online postings which include an implied or explicit affiliation with Castle may be removed if management deems them to be inconsistent with Castle's business interests or existing Castle policy. Messages in this category include: (a) political or religious statements, (b) cursing or other foul language, and (c) statements viewed as harassing others based on race, creed, color, age, sex, physical handicap, gender identity or sexual orientation. The removal decision must be made by a member of the top management team. When practical and feasible, individuals responsible for the message will be informed of the decision and given the opportunity to remove it themselves.

Intellectual Property Rights and Personal Use

Copyrights: Castle adheres to software license agreements. When at work, or when Castle systems are employed, utilization of software in a manner that is not consistent with the applicable license is forbidden. Open-Source licenses for third party libraries in use by Castle products must be respected. Reproduction or redistribution of words, images, or other copyrighted materials must be done only with the permission of the author or copyright owner.

Inappropriate Use: Exchange of information inconsistent with Castle's business (e.g. pirated software, stolen passwords or credit card numbers, pornography) is prohibited.

Personal Use: Use of Castle electronic resources for personal purposes is permissible so long as business activity is not hindered by the personal use. Employees must further not employ Castle information systems in such a way that the productivity of other employees is eroded.

Online and Privacy Expectations

Browser User Authentication: Castle account passwords should be stored using the Castle's Lastpass tool. When they must be saved in the browser, this should only be on a computer configured to require a login password each time it is turned on, and a screen saver password must be provided each time it is inactive for a specified period of time, as defined in the ***Network and Access Control*** policy.

Disallowing Access: Unless approved by management for business purposes, employees may not provide access to Castle systems (in the cloud or otherwise) such that non-Castle users gain access to internal Castle information.

No New Business Channels: Employees are prohibited from using Castle electronic resources to establish new business channels, such as e-commerce sites, cloud-based storage and similar services.

No Default Privacy Protection: Employees using Castle information systems should realize that their communications are not protected from viewing by third parties. Unless encryption is used, employees should not post or send information over the Internet if they consider it to be confidential or private.

Management Review: At any time and without prior notice, Castle management reserves the right to examine emails, files, browser cache files and logs, bookmarks, and all other information stored on or passing through Castle information systems, including end-user devices. Such management access assures compliance with internal policies, and assists with internal investigations and the management of Castle information systems.

Reporting Security Problems

Notification Process: If sensitive Castle information is lost, disclosed to unauthorized parties, or is suspected of such, the SLT must be notified immediately. If any unauthorized use of Castle's information systems has taken place, or is suspected of such, the SLT must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, inadvertently disclosed, or are suspected of such, the SLT must be notified immediately. Because it may indicate a virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must be reported to the IT dept for further handling. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

False Security Reports: The Internet is plagued with hoaxes alleging security vulnerabilities. Many of these hoaxes take the form of chain letters or Facebook postings requesting that the receiving party send the message to other people. Employees concerned about vulnerabilities should reach out to the SLT, who will then determine if any action is appropriate. Employees should not otherwise redistribute system vulnerability information.

Testing Controls: Employees must not probe security mechanisms at Castle or elsewhere unless authorized to do so as part of their normal job duties or have first obtained permission from the SLT.

Data Destruction

Any print, facsimile or other physical media, computer system, electronic device or electronic media disposed of, 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.

Appendix – Social Networking

Due to the popularity of social networking sites such as Facebook, LinkedIn and Twitter, Castle has established a policy around their use. This policy identifies standards regarding activities associated with such sites, including the posting of information, pictures, or other materials. Even though such sites are frequently used to express personal views, they can directly or indirectly impact Castle, other employees, partners or customers. Our approach emphasizes good judgment, common sense, courtesy and respect for customers, colleagues and others with whom Castle interacts or does business.

Given the unrestricted and public nature of the internet, there can be no expectation of privacy with respect to any information posted on such sites. We reserve the right to access or monitor the use of any publicly accessible information any employee may post on these sites, and expect employees to demonstrate respect for others when participating in or posting to them.

Additionally, it should be remembered that social networking sites may be reviewed, copied and distributed by others, including our competitors. At no time should any of Castle's trademarked, confidential, sensitive or proprietary information be posted on any social networking site without authorization from Castle management. If an employee is unsure whether the information they intend to post on any site is confidential or proprietary, they must contact and obtain explicit management approval prior to posting the information. Disclosures that violate the privacy, trade secret, intellectual property, or other proprietary rights of any individual or organizations, including Castle, are in direct violation of this policy. Always err on the side of caution.

Employees are not authorized to speak on social networking sites on behalf of Castle, unless given specific, prior approval from their manager or department. Such approval may be defined as continuous, such as when posting on social networking sites is a designated part of an employee's job duties. Employees should recognize that their online behavior may, even unintentionally, reflect on Castle. Castle expects an employee's behavior to reflect good judgment and professionalism at all times. Communications that are associated with or linked to the Castle, even indirectly or by innuendo, which disparage or exhibit disrespect for others are considered inappropriate.

Castle does not permit employees to take or disseminate images or depictions of our customers, partners, employees or facilities for any purpose that is not expressly authorized by Castle or without the express consent of those parties.

Finally, Castle is firmly committed to its equal employment opportunity policies. We do not condone or tolerate any form of unlawful discrimination regarding our customers, current or potential employees or other third parties. We also prohibit all forms of unlawful harassment, including harassment based on sex, gender, race, color, religion, national origin, ancestry, pregnancy, age, marital status, sexual orientation, gender identity, medical condition, veteran status, and physical or mental disability or any other characteristic protected by federal, state, or local law. Employees are prohibited from engaging in any conduct, activities, communications or postings that violate these principles. This includes using social networking sites to gain access to information about a potential employee that would otherwise be inappropriate to consider in the application stage (e.g. to determine an applicant's race, age, or gender identity) or using such sites to engage in behavior against other employees, customers or other third-parties that violates this paragraph or any state, federal or local law.