CYBER SECURITY POLICY

1. PURPOSE

Capstone Mining Corp. and all subsidiaries ("Capstone" or the "Company") are committed to achieving a targeted level of protection from internal and external cyber security threats, and accordingly, will implement ongoing governance, policies, and practices which address the following objectives:

- Ensure business continuity, including the recovery of data and operational capabilities in the event of a security breach.
- Ensure compliance with all applicable laws, regulations, and Capstone's policies, controls, standards and guidelines.
- Comply with requirements for confidentiality, privacy, integrity, and availability for Capstone's employees, contractors, vendors, and other users.
- Establish controls for protecting Capstone's information and information systems against theft, abuse, and other forms of harm or loss.
- Motivate administrators and employees to maintain the responsibility for, ownership of, and knowledge about information security.
- Ensure the protection of Capstone's data and information assets.
- Ensure the availability and reliability of the network infrastructure, systems and the services.
- Ensure that external service providers are made aware of, and comply with, Capstone's information security needs and requirements and continuously assess whether they maintain an acceptable cyber security posture.
- Balance the need for the above with the investment and policy constraints required to achieve an appropriate level of protection while maintaining business agility.

2. SCOPE

This policy applies to all permanent and temporary employees of Capstone Mining Corp. and all subsidiaries, and to directors, independent contractors, consultants, vendors, suppliers, agents, and other users of Capstone's IT resources (together referred to as "users") wherever they may be located. The policy is structured in the following categories:

A. Leadership and governance
B. Human factors
C. Information risk management
D. Business continuity
E. Operations technology; and,
F. Legal and compliance

Each site or operating unit can develop their own Cyber Security policy or policies that are adapted to local requirements that meet, at a minimum, the elements of this policy.

Any breach of this policy is a serious offence and will result in the consideration of appropriate sanctions up to and including termination of employment, contract or legal action.

3. DETAILS

A. Leadership and Governance

Cyber security is a strategic business matter for Capstone. It is not a technical consideration. The assessment and management of Cyber Risk is integrated into our Enterprise Risk Management System for the Company as a whole and for each of its separate operating units. Accordingly:

- The development and promulgation of a cyber security plan at the Company is the responsibility of the CFO.
- The implementation of the cyber security plan is the responsibility of operations and functional leadership who are accountable for the results.
- Oversight of the effectiveness of the cyber security plan is the responsibility of the Risk Officer.
- Cyber risk should be reflected in reports and updates to operations management, senior management as well as the Board of Directors of the Company at least quarterly.
- Cyber risk should be considered by all levels of leadership where changes to business processes, including but not limited to, the information and technology environment.

B. Human Factors

Authorized use: Capstone provides access to information technology to users, including the internal environment, the internet and social media, where relevant and useful for their roles within or for Capstone. Capstone prohibits use of IT resources for any purpose other than business, unless otherwise stated in this policy. All users must behave honestly with vigilance, respect the intended business use of technologies and comply with software licenses, property rights, user agreements, confidentiality, and legal rights. Users must comply with Capstone's Code of Conduct, Capstone's policies, and all applicable law when using Capstone's information technology resources, including without limitation privacy and intellectual property laws.

Limited personal use is acceptable provided that it does not affect job performance, is not for personal financial, commercial, or third party gain, and if the user adheres strictly to this policy. Capstone systems must not be used for the creation or distribution of any material considered inappropriate, offensive, threatening, abusive, defamatory, unlawful, sexually explicit, sexist, racist, discriminatory, embarrassing, fraudulent or disrespectful to others or that could potentially breach the corresponding software license agreement. Capstone restricts all users from using the Internet to perform any task contrary to the law or knowingly accessing websites with content that is illegal, obscene, hateful, defamatory, indecent, objectionable, or inappropriate.

To maintain the integrity of Capstone's corporate image and reputation and to prevent the unauthorized or inadvertent disclosure of sensitive, confidential or personal information, employees must exercise caution and care when using any system, service or technology platform, both internal and external, including email or third party services, such as Cloud-based and social media. Personally identifiable information, which is any data that could identify a specific individual, should not be transmitted via email or shared using any other service (with the exception of site level or corporate HR or legal groups) without approval by the appropriate site or corporate HR group. For clarity, a description of personally identifiable information is provided in **Appendix I**. Employees must also exercise caution against suspicious messages and technologies, which are often intended to bait a user into a malicious cyber event.

Passwords: Users are responsible for utilizing effective passwords and for keeping those passwords secret and secure. Employees must not appropriate, use or disclose someone else's login or password without prior authorization by the employee's supervisor or Human Resources. In addition, employees should ensure that the function of retaining passwords by company computers is disabled. The IT

Department will support the mechanisms that evaluate the strength of passwords and define the password change frequency for every type of applications, services and devices supported by the Company, along with other mechanisms to strengthen the way users identify themselves when accessing Capstone's IT resources, such as multifactor authentication. A guide to the development of acceptably effective passwords and the required frequency of change is provided in **Appendix II**.

Active Directory Accounts: Internal accounts used by Capstone personnel must have a unique User ID and password, and cannot be used by or shared with anyone other than the for whom it is intended. Personnel external to Capstone (i.e. consultants and/or contractors) should also be provided with unique user IDs and passwords, and follow the same internal controls relating to the granting and/or revoking of access as internal Capstone accounts.

Contractors, vendors and/or consultants must ensure all accounts/passwords assigned to them will be stored in a secure password vault.

The use of shared accounts (i.e. more than one person using a single User ID and password) is not permitted under any circumstance. Please see **Appendix V** for details on how to use SharePoint to provide controlled access to information to third parties (for example, to provide a team of consultants with project-specific materials). Use of SharePoint should be assessed, confirmed and/or decommissioned as part of regular IT internal control processes for granting / revoking systems access.

Active Directory constitutes the official corporate directory of users and it must reflect up to date information, including but not limited to, user's full name, department or functional area the user is associated with, direct reports, phone numbers, organizational position or role, etc. It is the responsibility of every department or functional area lead to ensure the information is current by advising Human Resources of any change. Corporate IT will provide the mechanism to enable this update process.

***Confidentiality*:** Capstone prohibits the release of confidential information to any third party, or use of confidential information, except as required in the performance of Capstone-related work approved by the employee's supervisor and in accordance with the terms of the applicable confidentiality agreement.

Privacy: Users should have no expectation of personal privacy in anything they create, store, send or receive by e-mail or when using any corporate application if they use equipment (e.g. mobile device, computers) owned or provided by Capstone. The nature of Capstone's business requires effective monitoring of activities on Capstone's network, including the conduct of users. Capstone reserves the right to review and collect all information contained in e-mails, whether or not stored solely in personal folders on the computer operated by the user, and in all equipment owned or provided by Capstone.

***Ownership*:** Data and employees' work and work products belong to Capstone, including all messages, sent or received regardless of the device or application used to produce, send or receive it.

***Security*:** Used unwisely, the Internet can be a source of security problems that can do significant damage to the Company. Users must:

- Apply best practices to prevent any form of computer virus, Trojan, spyware or other malware from being into the company's environment. A list of actions to prevent this from occurring which every employee must be aware is provided in **Appendix III**. While this list is not exhaustive, it is illustrative of the burden of care that every employee agrees to accept in helping ensure the security of the Company and its IT environment.

- Only access websites, applications or systems for which they have authorization, either within the company or outside it.
- Only use approved services for the uploading or sharing of company data. A list of approved sources is provided in **Appendix IV**. This list is not exhaustive and is subject to revision, so prior to using any such service not on this list, employees should confirm whether it is approved.

Awareness, Communication and Training:

New Employees: To mitigate the risk of unintentional disclosure of confidential information by employees, Human Resources will refer newly onboarded employees to this policy and will require formal acknowledgement that it has been read, is understood and will be applied.

New and Existing Employees: To mitigate the risk of unintentional disclosure of confidential information by employees, cyber security training and awareness sessions will be provided as an integral part of employee onboarding and ongoing employee development. In addition, acknowledgement of this policy, that it is understood and that the employee agrees to apply it will be included in the annual sign off along with the code of conduct.

Departures and/or changes in employment status: Upon a change in status, including promotion, transfer or termination of employment the applicable HR department is accountable for ensuring that the local IT leader is advised so that the employee's network and physical access privileges are modified as appropriate in a timely manner.

Third Parties: Third parties, vendors, suppliers, partners, contractors, service providers, or customers with connectivity to Capstone's internal network or access to Capstone's data must comply with this Policy and the policy governing system access by third parties attached as **Appendix VI.**

C. Information Risk Management

The Company will develop, maintain and periodically review for appropriate updates risk appetite statements that:

- Articulate its position with respect to cyber risk.
- Specifically address the degree of protection (as measured by a "cyber maturity index" or some other appropriate benchmark) that we are targeting and how we will measure it.

The Company will develop, maintain and periodically update as required, an inventory of major types of information and systems on the basis of criticality to the business. This list, on a priority basis, will be used to formally assess the degree of cyber protection that the company has, the target degree of protection as well as the plans that are in place to achieve the desired level as appropriate. The target level will reflect the nature of the information or application as well as the risk appetite defined above.

D. Business Continuity

Corporate IT is responsible for the development and promulgation of standards and guidelines for acceptable IT related business continuity and disaster recovery plans.

Business continuity and disaster recovery plans should be developed and aligned at two levels within the organization for each operating unit or office:

a. The application owner - normally the individual who is regularly the business process lead and is the person having authorized the deployment of the application, is responsible for developing a continuity plan for business applications.
b. IT is responsible for developing a continuity plan for the overall IT environment, including data backup and recovery.

E. Operations Technology

Data, applications, and networks, new software and IT equipment: To prevent the deployment of software and IT equipment that could compromise the security of the entire information technology infrastructure, the IT Department in Vancouver will establish standards for the development, acquisition, or installation and approval of all new software and major equipment purchases. No software should be installed on Company-owned devices unless approved by the employee's direct supervisor and the IT department. Capstone installs only properly authorized and licensed software and prohibits any installation or use of unauthorized, unlicensed or illegally-copied software.

Change Management: To protect from changes that could compromise Capstone's operations, the IT Department in Vancouver will enforce standards for the approval and deployment of changes to the information technology infrastructure and environment as well as the implementation of any new applications of any type. These standards, require, amongst other provisions, that all changes be appropriately governed and managed – and must be tested, documented, with cyber, business, technical and legal risk areas considered, and have user acceptance documented before being installed in the production environment. The approved deployment plan must include rollback and contingency procedures.

Viruses and Malware: To defend the company from computer viruses and malware, all computers and devices connecting to Capstone's infrastructure must be approved devices and have the standard, authorized anti virus and malware protection software installed. It is responsibility of the IT Department to keep this software updated and of users to report to the IT Department any sign of infection. To further enhance security, personal email is not to be accessed, either through the web browser or applications, on Company laptops or computers. It is acceptable to sync tablets and mobile phones to personal email accounts as these devices do not access the company network.

Remote Access: Users must secure their remote access credentials. 'Save Password' options should not be used. Users must assume remote networks, such as home based, public wireless hot spots, etc., are unsecure and therefore user should adhere to the best practices and procedures layed out by the IT Department, including, but not limited to the Bring Your Own Device (BYOD) described in this policy to prevent interceptions, eavesdropping, unauthorized access, or direct attacks that could risk the integrity of the overall network.

Lost Devices: To prevent the disclosure of confidential information in lost or stolen devices, the IT Department will implement encryption and other security mechanisms to dynamically protect Capstone's data. The user is responsible to take appropriate precautions to prevent damage to, loss or theft of any device issued to them or approved for use by them. Each employee must report immediately to their supervisor and to the IT Department any lost or stolen devices and any suspected or confirmed breaches of those devices. The IT department will take the required measures to wipe remotely, where possible, any Capstone data still hosted on the lost device. If user's device is lost, stolen or upon termination, the IT department will wipe the device which may include user's private information. It is not the responsibility of Capstone to recover any personal data or media from a lost or stolen device.

Bring-Your-Own-Device (BYOD): Users must agree to the Terms and Conditions of the BYOD Program in order to use personally-owned devices to access Capstone information and resources. The guidelines for the BYOD program are outlined in **Appendix VII**.

***Equipment*:** Users are responsible for the hardware assigned to them. Relocations and transfers of equipment must be approved by the IT Department.

***VPN*:** In order to protect corporate data while using public networks, the IT Department, where required, will provide and support secured remote access, including Virtual Private Networks (VPN). Only Company issued devices will be configured with VPN (or equivalent) access. Users with VPN credentials are responsible for maintaining their confidentiality according to the password provisions of this policy.

Incident management: To promptly respond to threats, users are expected to communicate information security incidents to the IT Department in accordance with the incident response breach policy. Security incidents include any violation of this security policy that compromises corporate data independently of ownership of the device. The IT Department is responsible for the channels and procedures that guarantee that security incidents are identified, contained, investigated, and remedied.

F. Legal and Compliance

Capstone will regularly assess developments within the company and in the environment, and ensure the promulgation of corporate wide policies for:

- Cyber security management
- Management of third party's access to company networks
- Other policies as required to ensure minimum standards of care are taken by the organization to protect against cyber threat.

Cyber risk will be monitored through the ERM system, audited through the ICFR, ITGC and Internal audit programs and be included in the ERM report communicated to the Board of Directors quarterly.

All material contracts should be reviewed by legal counsel as a matter of course and to ensure that the potential cyber risk assumed or created as a result is understood by management.

All contracts for the provision of cyber related services to the company should be reviewed by legal counsel to ensure that management has the understanding of residual risks for purposes of making relevant business decisions.

Issue Date:	February 16, 2016	**Authorized By:**
Review:	Annually	SVP&CFO
Revised Date:	October 26, 2020	

Appendix I

Personally Identifiable Information

Personally identifiable information (PII) is any information that can be used to identify, contact, or locate an individual, either alone or combined with other easily accessible sources. It includes information that is linked or linkable to an individual, such as medical, educational, financial and employment information. Examples of data elements that can identify an individual include name, fingerprints or other biometric (including genetic) data, email address, telephone number or social security number. Safeguarding company-held PII (and other sensitive information) is the responsibility of each and every member of the workforce. Regardless of your role, you should know what PII is and your responsibility in ensuring its protection.

Although society has always relied on personal identifiers, defining and protecting PII has recently become much more important as a component of personal privacy, now that advances in computing and communications technology, including the internet, has made it easier to collect and process vast amounts of information. The protection of PII and the overall privacy of information are concerns both for individuals whose personal information is at stake and for organizations that may be liable or have their reputations damaged should such PII be inappropriately accessed, used, or disclosed

PII can also be exploited by criminals to steal a person's identity or commit other crimes. According to FBI statistics, identity theft continues to be one of the fastest growing crimes and can cause both financial and emotional damage to its victims. Due to this threat, many governments have enacted legislation to limit the distribution of personal information.

The following list contains examples of information that may be considered PII.

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or title number and related information
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Sometimes, one or two pieces of information can be combined with other information to compromise someone's identity, even if the individual pieces of information seem harmless.

Appendix II

Tips for creating a strong password

Passwords provide the first line of defense against unauthorized access to your computer. The stronger your password, the more protected your computer will be from hackers and malicious software. You should make sure you have strong passwords for all accounts on your computer. If you're using a corporate network, your network administrator might require you to use a strong password**.**

What makes a password strong (or weak)?

A strong password:

- Is at least eight characters long.
- Does not contain your user name, real name, or company name.
- Does not contain a complete word.
- Is significantly different from previous passwords.
- Contains characters from each of the following four categories:

Character category	Examples
Uppercase letters	A, B, C
Lowercase letters	a, b, c
Numbers	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols found on the keyboard (all keyboard characters not defined as letters or numerals) and spaces	` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /

A password might meet all the criteria above and still be a weak password. For example, Hello2U! meets all the criteria for a strong password listed above, but is still weak because it contains a complete word. H3ll0 2 U! is a stronger alternative because it replaces some of the letters in the complete word with numbers and also includes spaces.

Help yourself remember your strong password by following these tips:

- Create an acronym from an easy-to-remember piece of information. For example, pick a phrase that is meaningful to you, such as **My son's birthday is 12 December, 2004**. Using that phrase as your guide, you might use **Msbi12/Dec,4** for your password.
- Substitute numbers, symbols, and misspellings for letters or words in an easy-to-remember phrase. For example, **My son's birthday is 12 December, 2004** could become **Mi$un's Brthd8iz 12124** (it's OK to use spaces in your password
- Relate your password to a favorite hobby or sport. For example, **I love to play badminton** could become **ILuv2PlayB@dm1nt()n**.

Appendix III

List of best practices to prevent any form of computer virus, Trojan, spyware or other malware infection

- Do not open emails from unknown senders.
- Don’t click on any links within emails that seem suspicious or from unknown senders.
- Don’t install any software on company issued computers without prior approval from IT Dept.
- Only open websites that you know. Never randomly click a link as it may direct you to a malicious website or trick you to download an infected file or program.
- When using USB flash drives, thumb drives or any other removable drives, make sure you scan them using your security software. Best practice is to ask IT dept. to scan if you’re not too sure.
- Limit the amount of information that is published on the internet about yourself or about Capstone. This can be used for social engineering.
- Report any suspicious computer activity to IT Dept. right away.
- Educate yourself on the protection systems that are installed on your computer and to check if it is up to date or any alerts.
- Never leave your computer unattended while outside the company offices where anyone could plug in a USB device. As a best practice always lock your computer session before leaving your computer unattended.

Appendix IV

Approved services for the uploading or sharing of company data

Approved Services provided by Capstone.

- Capstone's SharePoint
- Capstone's OneDrive for Business Online.
- Capstone's Dropbox for Business.
- Capstone's Email System.

Appendix V

Use of SharePoint and OneDrive to provide shared access to information with authenticated external users

Sharepoint and/or OneDrive may be used to share information / data; users should keep in mind disclosure and confidentiality considerations as materials on SharePoint and/or OneDrive can be downloaded / manipulated / distributed.

- A shared folder or file can be created and shared externally via Sharepoint and/or OneDrive and access granted to an authenticated external user.

Appendix VI

Provision of systems access to third parties

1. INTRODUCTION

From time to time, Capstone Mining Corp. and its subsidiaries (together "Capstone" or "the Company") may grant temporary and restricted access to their Information Technology ("IT") systems to authorized third parties for the purposes of implementing, maintaining or upgrading of applications and systems, or for assisting with specific projects. The engagement of third parties presents an inherent risk to Capstone's IT environment, which, if not appropriately mitigated, could lead to adverse business or cyber impacts. This Policy outlines how third party access to Capstone's IT systems will be controlled and limited to protect the integrity of Capstone's IT systems, to comply with contractual and legal obligations, and to safeguard Company information and operations.

2. SCOPE

This Policy applies to Capstone and establishes a process for granting and controlling third party access to IT systems and applications of Capstone.

a. The owner of an application or a system ("the owner") is the individual accountable for the integrity of that application or system as well as its output, and is responsible for determining when a third party requires access to that particular application or system and other complementary aspects of the Capstone IT environment. This owner may be a leader within an operations or functional group in the case of an application (e.g. The Director of Marketing for MineMan, the Pinto Valley Controller for E-SAP) or could also be a member of the IT group – either at site or corporate office in relation to infrastructure or IT environment issues.

b. The owner must prepare a request for access to be granted that should be approved by their direct leader as well as the Director of Information Technology or his designate before access can be granted.

c. Due diligence should be performed according to the following guidelines:

    i. The owner is responsible for the completion and documentation of the appropriate due diligence. This template does not cover financial, technical competence etc. and other traditional supplier/contractor due diligence steps the company would perform as a requirement of good business practices or other policies.

    ii. Any third party being granted access to any of Capstone's systems must sign:
        1. Standard form of confidentiality agreement
        2. Agreement to comply with Capstone's Cyber Security policy and Code of Conduct
        3. An acknowledgement that each user access will be unique and that individuals will not be permitted to share access rights, credentials or passwords.

    iii. Prior to being granted access:
        1. The owner should confirm there are no legal proceedings or threatened proceedings or judgements against the contractor that should influence our willingness to provide access.

2. The owner should specifically inquire about the contractor's practice of conducting legal background checks on its employees and whether there is anything that would influence our willingness to provide access.
3. The owner should inquire as to whether the contractor carries insurance that would otherwise protect the company against the contractor's activities or those of its employees, whether or not inadvertent or legal and make a decision as to how this should influence our willingness to grant access.

iv. The owner is responsible for verifying that:
1. The access granted is limited in scope and time period to the work for which it is necessary that the contractor or supplier has access.
2. That access has been revoked when appropriate.

d. The request must include:

i. Documentation supporting an appropriate level of due diligence on the individual or organization to whom access is to be granted has been completed.

ii. The specific access being granted, including the applicable applications, systems or aspects of the environment, the anticipated actions being contemplated by the third party through the granting of this access as well as either the time or result that will trigger that access being revoked.

iii. The business case for the specific access being granted.

Prior to gaining access, the third party must sign a document that comprises:

1. Capstone's standard non-disclosure agreement
2. Acknowledgement and agreement to adhere to all applicable laws and Capstone's policies as applicable to the services provided by the third party (including but not limited to Capstone's Code of Conduct, Cyber Security Policy)
3. Commitment to communicate to Capstone, which should be acknowledged, regarding any Cyber Breach that is experienced in the third party's network, systems or computers.

e. Each individual third party must have a unique active directory account established for them, including log in details and passwords. There should be no generic or global accounts or common log-in credentials or passwords.

f. The owner is responsible for notifying the local IT manager and the Director of IT in Vancouver as to when the conditions for revocation of access have been met or if circumstances warrant a change or extension of the access rights.

g. The owner is responsible for ensuring that access rights are revoked or modified as appropriate.

h. Access to Capstone's systems and/or IT resources will be only allowed using Capstone's computers or through Capstone's remote access service (https://connect.capstonemining.com/) or its local equivalent.

i. Access to local network resources or to the Internet will be granted only to the public/guest segment of Capstone's local area network.

Appendix VII

BYOD Guidelines

This appendix sets out the terms and conditions for the use of personally-owned devices (each a "device") that are authorized by Capstone Mining Corp. or any of its subsidiaries (together "Capstone") to access Capstone information and resources (together "Capstone Resources"), such as accessing Office 365 services and syncing Capstone e-mail on a device.

In this appendix, "devices" includes laptops, home computers, smartphones and tablets. "users" are all those individuals with an assigned individual Capstone account to provide access to any Capstone application or system and "including" means "including without limitation".

Users are not permitted to connect to or access Capstone's systems or network under the BYOD program using devices that are not approved by Capstone. Users must obtain the approval of the Corporate IT department before using any device to connect to or access Capstone's systems or network by contacting the Corporate IT department by telephone or e-mail at support@capstonemining.com. Capstone may deny access to enterprise systems, reasons for which may include the following: user's status, user has sufficient access through Capstone-issued devices, or user works with sensitive information (including personal information or confidential information). For greater certainty, provided that users comply with these terms, users do not need prior approval of the Corporate IT department to access Capstone Resources, such as accessing Office 365 services from a home computer or syncing Capstone e-mail on a device.

Terms to Use of Devices

1. Users agree that in exchange for using their personal devices for business purposes, they will give up control over their devices and comply with these terms and any requirements as required by Capstone from time to time, including as applicable: meeting specified encryption or password standards; permitting Capstone to monitor use of personal information in Capstone's control on user's device; permitting Capstone to reset or wipe the device clean (i.e. in its entirety, including both 'business' and 'personal' data) including in the circumstances described in clause 5 below; promptly downloading, installing, loading, updating, upgrading or removing certain applications or system software as required by Capstone from time to time; and upon Capstone's request, allowing Capstone to download, install, load, maintain, update or remove a mobile device management software agent or any other software deemed necessary on user's device. **Capstone will not be held liable for erasing user's applications and content (including any personal application and data) or in connection with the installation or updates of any software on the device for any reason**.

2. All devices permitted to be used in connection with the BYOD Program will remain the property of the users.

3. Users assume all risks and full responsibilities in connection with the use of their devices, including users' personal content on the devices, the backing up of any personal content (applications and data) on the devices, and all costs related to each device (including the purchase cost of the device, upgrades or repairs to the device, and any fees with the

telecommunication service provider). Capstone is not responsible in any way for users' devices for any reason, including any lost or stolen devices or charges relating to usage.

4. User's device must satisfy the following minimum requirements as required by Capstone from time to time. The minimun requirements will determine the specifications that an approved device must meet, including, but not limited to:

    a. Software licenses for all the applications installed.
    b. An antivirus/anti-malware protection up to date.
    c. Strong password(s) and/or biometric authentication.

5. Users agree that Capstone may do all things necessary to protect Capstone Resources, including remotely wiping all data and applications on the user's device when viewed appropriate by Capstone (e.g. if the device is reported lost or stolen, or if the user is no longer employed at Capstone, or if there is a security breach in connection with the device).

6. User must take appropriate precautions to prevent loss or theft of the device, and to prevent others from obtaining unauthorized access to the device (including sharing passwords or other credentials to enable access to Capstone Resources, or sharing use of the device with any person).

7. If the device is lost, stolen or may be compromised in any way, or if user plans to replace, discard, or update his or her device, user must immediately notify Help Desk. If applicable, prior to any cancellation of mobile services associated with the device or prior to changing the device, user must allow Capstone IT to remotely wipe the device.

8. Users will bring their device(s) to Corporate IT (or site IT as applicable) for physical security assessments or as required by litigation or other legal purposes, and will hand over necessary device access codes upon request.

9. Users will comply with all Capstone policies and applicable laws when connecting their devices to Capstone Resources, including the Cyber Security Policy and Privacy Policy.

10. Non-compliance with these terms and conditions may result in revocation of user's right to use the device for business purposes, and may result in internal disciplinary action up to termination of employment with cause or termination of consulting arrangements without notice and without compensation where permissible under applicable laws.

11. Use should not expect any commitment from Capstone to configure, troubleshoot, repair or replace any BYOD device.

Appendix VIII

RACI MATRIX[1]

This appendix sets out the responsibilities for all roles involved in Capstone's Cyber Security program and aspects described in this policy. This appendix uses a Responsible, Accountable, Consulted and Informed (RACI) Chart as a planning tool to help establish what needs to be done and who must do it. R-A-C-I stands for the different expectations of team members. A description is provided below for the role of each category—those responsible, accountable, consulted, or informed for an activity or decision within the context of this Cyber Security Policy.

	Board of Directors	**CEO**	**CFO**	**IT**	**Information Owners (Business** Process	Senior Vice President Legal, Risk & Governance	Cyber Security Team	**All Employees & Contractors**	Human Resources
Define the risk tolerance level	A	C	C	R	C	C	C	I	-
Cyber Security Plan Develpment	C	C	A	R	C	C	C	I	-
Cyber Security Plan Oversight, Identify and monitor for risks	I	I	I	R	I	A	R	I	-
Perform comprehensive system-wide risk assessments	A	C	I	R	-	R	C	-	-
Perform per-project or initiative-based risk assessments	I	I	I	A	C	I	C	-	-
Evaluate and identify risk actions	I	I	I	A	C	I	R	-	-
Approve and fund risk actions	C	A	R	C	I	-	-	-	-
Manage and maintain IT risk register/inventory	I	I	I	A	I	R	C	-	-
Capstone's Accounts Directory (AD), user onboarding/offboarding & changes	-	-	-	R	C	I	I	-	A
Personally Identifiable Information	-	-	-	R	C	I	I	-	A
Cyber Breach	I	I	C	A	I	C	C	I	-

1

RACI		Description	How Many in This Role for a Decision?
R	Responsible	Makes sure things get done	Usually one (but sometimes more)
A	Approver	Makes the decision	One
C	Consulted	Makes recommendations	Varies (0 to many)
I	Informed	Get informed of the decision after it is made	Varies (0 to many)