Contents

1. Purpose

This Written Information Security Policy (“WISP”) is a representation of the standards established across the business areas and all associated group entities (“CR”) to ensure the confidentiality, integrity, and availability of CR data. The procedures and guidelines set forth in this WISP were developed to ensure CR confidential data remains protected in a manner that is consistent with the Company’s standards. Protecting the systems in which CR confidential data is processed, stored, or transmitted is of equal importance to the Company. As such, any reference to confidential data in this WISP includes the Company’s systems.

2. Scope

This policy applies to every employee and contractor (worker) of CR who uses CR’s ICT Systems. It applies at the workplace and when workers are working for CR away from the workplace. It also applies to use of CR’s ICT Systems and equipment outside of working hours or away from the workplace (such as at home).

3. Governance

The Information Security Team (see **Appendix A** for details) is responsible for administering the Company’s WISP. The Information Security Team may delegate certain duties to another qualified employee(s). Therefore, any reference to the duties of the Information Security Team shall include any designated employee(s). The Information Security Team’s duties include, but are not limited to:

- Distributing this WISP to employees and providing training to employees based on this WISP.
- Responding to employee inquiries as they pertain to this WISP.
- Overseeing the Company’s cybersecurity program and leading incident response efforts.
- Monitoring for cybersecurity-related legal or regulatory developments.
- Coordinating with management, IT personnel, and/or legal counsel to discuss cybersecurity-related issues or topics.
- Reviewing and updating this WISP, as necessary or on an annual basis.
- As part of CR’s commitment to continual improvement, this document will be reviewed and updated, as necessary or on an annual basis.

4. Responsibilities

Responsibilities of IT

The CR IT Department manages the IT network and systems in which the Company operates. The IT Departments responsibilities are specified throughout this WISP. In general, the IT Department’s duties include, but are not limited to:

- Configuring systems and controls based on the Company’s standards
- Monitoring and maintaining the Company’s IT network and infrastructure
- Managing the maintenance and development of all CR IT platforms
- Providing first point of contact and support during critical incidence or data breach incident – Refer ITP-07 CR Cyber Security Incident Response Plan and ITP-05 CR Data Breach Management Policy.

Responsibilities of CR Digital

The CR Digital business unit manages the deployed systems on customer mine sites that do interact with the CR IT network and systems in which the Company operates. The CR Digital department responsibilities are in addition to the IT responsibilities and are to ensure that customer data is managed appropriately. It includes ensuring:

- Configuring customer systems and controls based on the Company's standards
- Monitoring the Company's production infrastructure
- Monitoring the administration of API's (inbound and outbound)
- Managing customer user specific credentials

Responsibilities of Workers

It is the responsibility of workers to:

- Understand the requirements of this policy and to seek further information if unclear.
- Comply with the requirements of this policy and consider this policy in all requirements of your role including Project Management
- Report immediately to their manager, The IT Department or The Information Security Team any breaches or potential breaches of this policy, whether deliberate, reckless or accidental.

Responsibilities of Managers Roles and Responsibilities for Information Security

Information Management Systems Steering Committee is defined in the CR ISMS Framework document and CR Information Security Management System Terms of Reference.

The Senior Management are ultimately the owners of all information security risks. The Senior Management will have the authority to:

- Mandate, through the Information Security Policy the establishment of an ISMS which is compliant with ISO27001:2022
- Assign additional roles and responsibilities for the management of information security within CR
- Establish the ISMS Committee to govern the ISMS

The ISMS Committee is responsible for the information security management of CR's information. The day-to-day management of the ISMS and key responsibilities are assumed by CR's Head of IT.

All staff and contract employees are responsible for knowing and following CR's policies and procedures.

All staff are also responsible for enforcing and observing the security controls implemented by CR. In the absence of formal security policies or procedures, all staff must adhere to best practices such as those prescribed in ISO 27001:2022 or as agreed with the ISMS Committee.

All staff are also responsible for reporting security events, potential risks, control defects, opportunities for improvement, breaches and suspicion of breaches to the ISMS Committee.

Managers (or staff in management and leadership positions) must actively enforce information security policies, procedures and controls within their organisational scope and escalate any non-compliance to the ISMS Committee.

5. User Awareness and Training

All CR users with access to CR platforms must complete Cyber Awarenesss training as provided by HR and IT, initially to employees upon hire (as part of the onboarding process) and on an annual or as required basis through their employment with CR.

Cyber Awareness training may address a variety of topics relating to this WISP, cybersecurity events recently in the news, common phishing techniques, how to identify red flags, and other topics deemed relevant at the time of the training.

CR will provide regular Cyber Awareness training including monthly videos and quiz questions directly from the Mimecast platform. CR will distribute regular test phishing emails in order to track user click rates and user diligence around reporting of suspicious emails. A monthly report will be generated and delivered to the HR team to assess if further training or security education requirements. Disciplinary action may be taken if users are deemed to be in continuous breach of the CR awareness training policy requirement for example, ongoing failure to complete awareness training or ongoing failure of phishing tests.

6. Information and Asset Classification

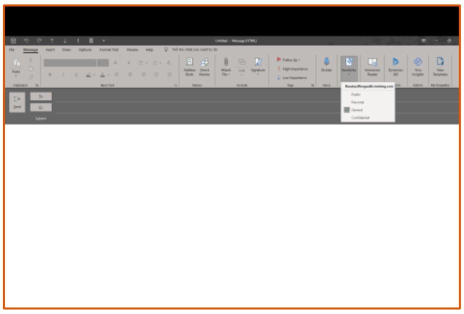
Employees must understand CR’s criteria for what is deemed confidential in order to appropriately manage CR’s data. The table below categorizes CR data to provide employees with an understanding of the types of data classified as confidential at CR. The data identified below is not an exhaustive list of the types of data CR maintains, is responsible for, or manages. To reduce the possibility for errors, any data not specifically classified below, created at CR, or received by CR employees in the performance of their jobs should be treated as confidential.

Category:	Definition:	Impact	Examples
Confidential Data	**Definition: Highly valuable, highly sensitive data/asset that could adversely affect CR if it were made available to the public.**	**Potential Impact of Loss: Impact may negatively affect CR**’s **competitive position, violate legal or regulatory requirements, violate contractual requirements, damage** CR’s **reputation, and cause financial loss.**	▪ **Personally Identifiable Information (PII)** ▪ **Business Plan & Marketing Strategy** ▪ **Financial Data Related to Revenue Generation & Budgeting** ▪ **Username & Password Combinations** ▪ **Hardware or Software Tokens (multi-factor authentication)** ▪ **System Configuration Settings** ▪ **Regulatory Compliance Data** ▪ **SEC Disclosure Information** ▪ **Third-Party and Employee Agreements** ▪ **Strategic or Operating Financial Data** ▪ **Corporate Tax Return Data** ▪ **Electronic Payment Data (Wire Payment/ACH)** ▪ **Pay slips** ▪ **Incentives or Bonuses (amounts or percentages)** ▪ **Stock Dividend Data** ▪ **Bank Account Data** ▪ **Investment-Related Activity** ▪ **Account Information (e.g., stocks, bonds, mutual funds, money markets, etc.)** ▪ **Debt Amount Information** ▪ **Unannounced Merger & Acquisition Data** ▪ **Intellectual Property** ▪ **Legal Documentation & Billings** ▪ **Trade Secrets (e.g., design diagrams, competitive data, etc.)** ▪ **Information about current customers or suppliers of CR.**
Internal Data	**Definition: Data/asset that has been approved for release to approved business unit user groups but is not generally public across all business unit users,**	**Potential Impact of Loss: Impact would be damaging or pose a risk to business operations. Information shared across unauthorised users through extraction to excel or other format or password sharing may negatively affect CR competitive position, risk unapproved employees to view sensitive information.**	▪ **Competitive pricing across international customers, wage detail or summaries, etc.** ▪ **Internal IP Addresses** ▪ **Marketing Promotions In-Development** ▪ **R&D Activity**
Public Data	**Definition: Data/asset that has been approved for release to the general public or is generally available to the public.**	**Potential Impact of Loss: Impact would not be damaging or pose a risk to business operations.**	▪ **Internet-Facing Websites (e.g., Company website, social networks, blogs, etc.)** ▪ **Approved Press Releases** **Financials lodged with ASIC**
Assets	**Definition: Assets relate to IT hardware distributed for use by**	**Potential Impact of Loss: Impact would not be damaging or pose a risk to**	Criticality A

	employees, (laptops, servers, printers etc) but also include software, Databases and CR information, office infrastructure and outsourced services such as ShareFile, Box.com,	**business operations. Assets listed come under Criticality D – No impact either because of redundancy or not directly involved in the process.**	**Shuts down the entire plant, multiple production lines, safety & / or environmental reasons, equipment affecting multiple zones or areas, or equipment causing chains of events that cannot be controlled in time. Equipment classified as highly profitable or with high customer service needs or high volume demands. Equipment with high repair cost when they fail.** Criticality B **Some reduced capacity, equipment that can be bypassed economically for a period. Components on a single line.** Criticality C **Comfort items (HVAC, air make-up units, etc.)** Criticality D **No impact either because of redundancy or not directly involved in the process.**

7. Labelling Information

CR platform users are provided with an inbuilt MS Office 365 applications sensitivity labelling option for all new emails.



Confidential information should be labelled prior to sending. The responsibility for labelling confidential information is the creator of information. Terms of confidentiality with this policy may be superseded by other written agreement or non-disclosure terms.

Where information is considered sensitive, data masking shall be considered by CR using pseudonymisation or anonymisation techniques available from the service providers *e.g., encryption, value hashing, and substitution.*

All other correspondence should be marked accordingly: Public, Personal, General.

8. Access Controls

Access Rights & Administration

This policy is provided to maintain an adequate level of security to protect data and information systems from unauthorized access and defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of information systems.

Only authorized users are granted access to information systems, and users are limited to specific defined, documented and approved applications and levels of access rights. CR allow 'by exception' access to local admin for users that apply for, and have approved by their manager, local admin access. Local administrators are monitored as is their ability to download applications, both Mimecast and Crowdstrike provide alerts for any untoward application downloads. SSO has been applied to cloud services and MFA is CR's primary authentication method. The majority of staff are disallowed access to download or save to USB devices. Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability.

Who is Affected:

Access rights affect all employees of CR and its subsidiaries, and all contractors, consultants, temporary employees and business partners. Employees who deliberately violate this policy will be subject disciplinary action up to and including termination. *(Ref: PRO-0045 CR Code of Conduct)*

Affected Systems:

This policy applies to all computer and communication systems owned or operated by CR and its subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

Entity Authentication: Any User (remote or internal), accessing networks and systems, must be authenticated.

The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes but is not limited to:

- Automatic logoff
- Unique user identifier
- Multi Factor Authentication
- Password

Company Device Access Control System:

All workstations, laptops or other device used for this business activity, no matter where they are located, must use an access control system approved by IT. In most cases this will involve password-enabled screensavers with a time-out-after-no-activity feature. Active workstations are not to be left unattended for prolonged periods of time, where appropriate. When a user leaves a workstation, an automated lock screen policy will activate after 10 mins.

~~Access for Non-Employees:~~ Contractor or Third Party Management for System Access

Individuals who are not employees, contractors, consultants, or business partners must not be granted a user-ID or otherwise be given privileges to use the computers or information systems unless the written approval of the Department Head (Business General Manager) has first been obtained.

Before Contractors, third-party or business partner access to computers or CR information systems will follow the below process:

- A non-disclosure agreement defining the terms and conditions of such access must have been signed by both parties or a responsible manager at the third-party organization.
- Access requests to be submitted to the IT Service Desk
- A user account will be issued including a unique user id and temporary password.
- Granting permission to folders on the network based on the contractor’s job role and requested by the one-up manager.
- MFA will be mandatory for all third party, contractor or business partner access.
- Provided copy of CR Written Information Security Policy.
- The hiring Manager of the contractor to advise IT when the contractor term is completed to ensure access is disabled immediately

Unauthorized Access: Employees are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. System privileges allowing the modification of ‘production data’ must be restricted to authorised personnel provided access to ‘production’ applications for this specific purpose.

CR general data is stored on the Company’s network drive. Individual folders are maintained within the network drive based on the Company’s various business operations, controlled documentation is maintained in the MyOsh platform with access controls being maintained by the HSEQ team.

CR IT Department must obtain their direct Manager’s approval prior to enabling, modifying, or disabling access rights to the Company’s folders, applications, or any other systems containing confidential data. Access rights are reviewed regularly to ensure access has been appropriately granted and restricted from employees as necessary

Local Administrator Rights:

Local Administrator rights are restricted for CR employees. Users needing Local Administrator Rights to their device for the purposes of carrying out daily duties can submit a detailed purpose description to the IT Services help desk with one-up manager approval. These requests will be reviewed by IT and where necessary the CR ISMS

Committee prior to approving. Approved Local Administrator rights will be managed through CR security group policy and by exception only.

Requests for Administrator assistance can be submitted to IT Services.

.

9. On-boarding & Off-Boarding Policy

On-Boarding

The Company's employee on-boarding process includes, but is not limited to:

- Conducting a background check prior to employment for relevant staff levels and roles. (refer: *HR for Guide to Background checks*)
- Executing a confidentiality/non-disclosure agreement.
- Training new employees on the Company's policies and procedures.
- Creating user accounts for new employees and issuing each employee a unique user id and temporary password.
- Granting permission to folders on the network based on the employee's job role.
- Issuing a desktop and/or laptop computer.
- Ensuring email access is set up on the new employees' company issued mobile device.
- Issuing a key card for building and office access.

Off-Boarding

The Company's employee off-boarding process includes, but is not limited to:

- Disabling (i.e., password change) or deleting accounts promptly upon notification of termination or on the date of departure
- Ensuring employees return all Company property.
- Revoking email access on employee mobile devices.
- Revoking building and office access.
- Requiring employees to review and re-attest to their confidentiality/non-disclosure agreements.

Departmental Transfer

The Company's employee Department Transfer process includes, but is not limited to:

- Disabling (i.e. password change) or deleting accounts promptly upon notification of transfer or on the date of departure.
- Adjustment of data access security levels.
- Adjustment of email access on employee mobile devices (if applicable).
- Adjustment of building and office access (if applicable).
- HR to review and re-attest to their confidentiality/non-disclosure agreements.

Procedure reference: PRO-1294 Recruitment, onboarding, internal movements and offboarding procedures

10. Teleworker / Remote Access

Remote Access

The Company's network is remotely accessible via VPN for specific access to corporate platforms. Hosted platforms such as MS D365, ConnX and Inlogik can be access through an internet connection provided the CR URL, CR credentials with multi-factor authentication (MFA) are used.

Employees should save all documents on the Company's network or provided One-Drive folder during remote sessions, it is the responsibility of each employee to ensure data is not saved to the local laptop or desktop drive, local drive are not backed up by the IT Department. It is recommended that One Drive should be used for working documents. .

Email Access

Emails are hosted on MS Office 365 and each employee is issued an individual email account. Emails are accessible through Outlook Web Access (OWA) and multi-factor authentication (MFA) is required in order to access.

Employees should not log in to their Company email accounts from OWA on a public or non-Company computer. If there is a circumstance that OWA is used on a public or non-Company computer, documents or attachments should not be downloaded during the OWA session it is recommended that an incognito browser session be used.

11. Acceptable Use

Definitions

The following definitions are provided to assist workers and managers in understanding the acceptable usage policy.

ICT Systems covers all business applications, servers, networks, digital information and end user devices, including but not limited to, Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Area Networks (WLANs), intranet, internet, e-mail, computer systems, software (including software as a service), servers, desktop computers, laptops, tablets, printers, telephone systems, telephones, smart phones, digital cameras, video conference equipment, hand held devices

Use of ICT Systems and Devices includes, but is not limited to the following use:

- e-mail
- Instant messaging (SMS)
- Voice mail
- Social networking sites (e.g. Facebook, X)
- Professional networking sites
- Video and photo sharing websites
- Corporate Document sharing websites (ShareFile, Box.com)
- Virtual Data Rooms Browsing and publishing on the intranet
- Downloading or accessing materials from the internet or other electronic devices
- Web and video conferencing
- Podcasting and vodcasting
- Online discussion groups and chat facilities
- Subscriptions to work relevant , mailing lists, websites or other like services
-

Hotspotting from work provided phoneGeneral Requirements for Use of CR's ICT systems and Devices

Workers are provided with access to CR's ICT Systems to enable them to carry out business functions of CR efficiently. Workers are required to treat CR's ICT Systems with reasonable care, behave responsibly and not violate any legal requirement or the rights of others.

All workers using CR’s ICT Systems are required to comply with this policy and are required to comply with all laws, including, but not limited to, laws relating to copyright, anti-discrimination, defamation, harassment, misuse of information and criminal activities.

CR Proprietory Information stored on electronic and computing devices whether owned or leased by CR, employee or a third party, remains the sole property of CR.

If a worker becomes aware that CR’s ICT Systems and/or Devices are damaged, lost or stolen, the worker must report the matter immediately to management and contact a member of the IT team who will disable the account and take steps to protect any data that be impacted.

CR reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietory Information:

- All computing devices must be securerd with a password protected screensaver with automatic activation feature set at a global systems level.
- Postings by employees from an email address to newsgroups will contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of, unless posting is in the course of business duties.

> *“The information contained in this e-mail is confidential, may be legally privileged and is intended solely for use by the individual or organization to whom it is addressed. E-mail information is subject to copyright and cannot be used, disseminated, copied or disclosed to third parties without the written consent of CR. The views expressed in this e-mail are the views of the individual and may not reflect the views of CR. CR accepts no liability for any losses or damage arising from reliance on the information contained in this e-mail. If you are not the intended recipient please notify us immediately, delete this e-mail and destroy any copies.”.*

- Employees should use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. If unsure of content contact, IT Services.
- Email accounts provided by CR should be used primarily for company related purposes, personal communication is permitted on a limited and reasonable basis (refer section 9.4 Personal Use). The disclaimer included in postings to newsgroups will also apply to all outbound email correspondence.
- Email that is identified as CR business record shall be retained in accordance with the CR retention schedule.
- Users are prohibited from using third-party email systems and storage i.e., Google, Gmail, Yahoo to conduct CR business or to create or record any binding transactions. This includes using these systems to distribute any data related to a worker’s job even if distributing data to yourself.

Cryptography

- Cryptographic controls are implemented across CR on a risk-based approach that considers the sensitivity of CR information that the controls are planned to protect. Cryptographic controls do not alter the sensitivity of the encrypted information and will limit the ability of the information to be accessed by an attacker.
- Cryptographic key management for CR considers the sensitivity and criticality of the information the cryptographic key protects and dependent of key requirements are for data in transit or at rest and the duration of the cryptographic key life.

Details of the CR Cryptography and key management procedures are documented in ITP-01 CR IT Standard Operating Procedure.

12. Unacceptable Use

The following activities described below are, in general, prohibited. The lists below are by no means exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use. To the extent that a worker or manager is unsure whether an activity may be deemed to be unacceptable please check with IT.

System and Network Activities The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which or the end user does not have an active license is strictly prohibited.

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any CR account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using CR email to create or distribute any disruptive or offensive messages around race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs or political beliefs.
- Participate in any form of behaviour that would reasonably offend, humiliate or intimidate another.

13. Personal Use

Workers can use CR’s ICT Systems for limited personal purposes where this does not interfere with the performance of their duties or cause any material wear and tear on those Systems.

CR defines limited personal purposes as:

- personal e-mail
- online banking
- travel bookings
- limited web-browsing

Personal use means all non-work related use of CR’s ICT Systems and Devices, regardless of the usage location (e.g. onsite, at the office or at home) and the time of use (i.e. within or outside normal office hours).

Permitted uses do not include activities that would expose CR to legal liability or uses requiring substantial expenditures of time, uses for profit or uses that would otherwise violate CR’s policies with regard to employee behaviour, time commitments or CR’s equipment.

Use of CR applications on personal devices are not recommended and may be blocked via secure group policy – for example – access to CR MS Office 365, CR MS applications and MS One-Drive.

14. Equipment Siting and Protection

CR employees must minimise risk of damage, theft loss and compromise of CR assets including:

- Protect assets to reduce the risk of unauthorised access, environmental threats and hazards.
- The IT team must ensure that infrastructure is designed in a way to safeguard sensitive information and assets (i.e. secure comms room and restricted access).
- Employees should ensure monitors are angled to prevent unauthorised persons observing the display where possible.
- Autolock for all CR users will activate after 10 minutes.

- Printers, scanners and copiers must not be located in an area that is accessible to the public.
- Where possible access to CR offices will be monitored by way of a swipe card access system, other protections exist for visitors and contractors that visit CR offices.

15. Assets – Chain of Custody

- CR assets chain of custody will be managed by IT as follows:
    - Asset tagging the device prior to distribution
    - Employees will be granted only the privileges required to fulfill their tasks **(and approved by the hiring manager).**
    - Assets will be set up by IT including secure VPN access to the CR network and platforms.
    - Data and records will be managed by the users as outline in this document.
    - Appropriate data sanitization, backup or removal will be managed by IT on advice that a users is leaving the company.
    - If requirement reports and certificates of data destruction will be maintained by the IT Department.
    - All assets will be tracked through the Manage Engine Asset management tool.
    - Asset inventory will be reviewed on a periodic basis – minimum annually
    - The IT Department will ensure all devices are disposed of in a safe and environmentally-friendly manner.

16. Removal of Assets

CR owned equipment must be maintained in accordance with the Acceptable use procedure outlined in Section 10 of this policy.

- CR employees are not required to provide documented permission to remove issued equipment from an office site given CR supports working from home and travel to customer and work sites.
- CR employees must minimise risk of damage, theft loss and compromise of CR assets whilst travelling away from the office and ensure equipment is returned in the condition it is provided (excluding aging and accidental damage).

17. Security of Equipment and Assets off-premises

- CR owned equipment must be used in accordance with the Network and System procedure outlined in Section 20 of this policy.
- Access to the CR platforms through authorised control mechanisms such as passwords.
- Do not leave equipment unattended in a public area.
- Ensure CR equipment is under your direct control when travelling.
- Report accidental damage or theft of equipment immediately to the IT Department.

18. Asset Ownership

- IT Assets remain the property of CR, with staff members being custodians of that asset during their period of employment.
- The ownership of assets remains with the IT Department to track and manage distribution, asset tagging, software installation and return of assets to the IT Department.

19. Asset Disposal

The Asset owner should coordinate the decommissioning and disposal process, ensuring compliance with applicable laws and regulations.

Prior to disposal, Assets that may contain CR sensitive information should be sufficiently obscured, erased, destroyed, or otherwise rendered unusable.

Prior to destruction, Assets should be stored in a secure area.

In practice, the physical disposal of an Information Asset may be conducted by the IT team or outsourced to an external service provider that specialises in Asset disposal services.

Asset disposal should adhere to approved procedures and/or change management processes, including any required updates to the Asset register.

20. Clear Desk Policy

The CR Clean Desk Policy is an important tool to ensure that all sensitive or confidential data and hardware are either removed or locked away from a user's workspace.

Purpose

The purpose of a clean desk policy is to establish minimum requirements for maintaining a clean desk free from sensitive or critical information and maintain privacy for CR employees, CR's intellectual property and, CR customers and vendors.

Scope

The below policy requirements apply to all CR employees and affiliates whilst working.

Policy Requirements

- Secure all sensitive, restricted and confidential information, hardcopy or electronic format in a lockable drawer or cabinet if expected to be away from your desk for an extended period of time or prior to leaving the office at the end of a workday.
- Keys used for access to lockable cabinets or drawers must not be left at or around an unattended desk.
- Workstations and laptops must be locked when your workspace is unoccupied.
- Workstations and laptops must be shut down completely at the end of a working day.
- Laptops must either be taken off site at the end of a working day or locked away in a drawer or cabinet.
- Passwords must not be left on sticky notes or posted on any part of your desk or other accessible location.
- Printing of restricted or sensitive data should printed via the printer's secure print option and be immediately removed from the printer.
- Disposal of restricted or sensitive physical data should be shredded or placed in the locked confidential disposal bins.
- Meeting room and collaboration area whiteboards containing restricted or sensitive data should be erased immediately on close of the meeting. Where information is required to be left on whiteboards, please ensure that these whiteboards are in the secure areas of CR offices.
- All mass storage devices unless approved for use, should not be used to store CR data. If approved for use treat all mass storage devices as sensitive and store in a locked drawer or cabinet.

Policy Compliance

CR will verify compliance to this policy through various methods including but not limited to:

- Periodic office walk throughs.
- Internal and external audits.
- Yearly refresher training.

21. Electronic Message Monitoring

Electronic Communications Are Records Of CR

CR may be required to produce electronic communications to comply with the requirements of the law. Electronic communications are subject to any CR’s document storage procedures. This includes personal messages sent using CR’s ICT Systems and Devices. Workers need to be aware that electronic communications during the course of employment are the property of CR and may be accessed at any time.

Monitoring

CR may engage in the monitoring of digital messages, internet access, other electronic communications or files created by workers and the use of ICT Systems and Devices provided by the organisation. This may be done for security and network management reasons as well as to monitor for any unlawful activity or reasonably suspected policy breach. Monitoring can also be used to determine whether any worker is accessing, circulating, uploading or storing offensive or inappropriate material.

Monitoring of CR’s ICT Systems and Devices may also occur for the purposes of worker supervision or investigation purposes. All workers are taken to have consented to such monitoring upon their employment / engagement.

Suspect Material

Any e-mail or other material received by a worker that appears to be of dubious origin or source or contains questionable or offensive material should not be opened. Instead, the worker should report it directly to the IT Department and follow any instructions of the IT Department.

The worker should retain a copy of such material for the IT Department to review. Where this is not possible, the worker should record and provide details to the IT Department describing sender and receiver’s details, the type of material/ subject matter, the time and date received.

Malware

Email and web searches are potential access points for downloading computer malware. Employees are responsible for checking suspicious incoming email content or possible email scams. Items to look for are spelling and grammatical errors in the body of an unknown sender email, emails coming from unknown or unusual email address, links embedded in email text with any sense of urgency to ‘click and collect’ or ‘click and complete within 24 hours’. End user are provided with a pre-installed anti-virus protection application that should maximise protection, however this will not completely prevent users clicking links or downloading suspicious files. If in doubt users should provide information to IT Services for checking. It is better to STOP and delay a task than to be the cause of a serious data breach.

Blocking of Electronic Communications, E-mail or Websites

There may be circumstances where a worker’s access to electronic communications, e-mail and /or internet is blocked. Access to electronic communications, e-mails or internet will be blocked in the following circumstances:

- If an e-mail or other electronic communications is believed to be ‘spam’.
- if the e-mail, other electronic communications or website could interfere with or damage the CR’s computer, computer network, any program or data (e.g., an e-mail containing a virus).
- if the e-mail, other electronic communications, an attachment or website may be considered discriminatory, bullying, threatening, menacing, harassing or offensive.
- if the e-mail, other electronic communications, an attachment or website is unlawful or in breach of any policy of CR.

Electronic Security

Information generated by workers during the course of employment/engagement is owned by CR and must be stored and protected as CR requires. Workers must not deny access to these documents with a password that only they know. If workers need to password-protect a document due to work-related confidentiality reasons, then they must provide the password to the system administrator or their manager.

All workers are responsible for exercising good judgment when managing CR confidential data and systems. For security and network maintenance purposes, CR reserves the right to monitor workers activity on the Company's network at any time. If, at any time, a worker is uncertain of the proper procedures to follow when handling and storing confidential data, they must consult with the Information Security Team.

General Guidance

- Never reveal account passwords to others or allow others to use your account.
- Exercise caution when discussing confidential data over email, phone, facsimile machines, or messenger services.
- Exercise caution when mailing or faxing confidential data – a-controlled document sharing application is available for sharing confidential information – request access through ITService@crmining.com

Access Restrictions

- Any attempt to disable or circumvent any security settings configured on Company computers used for business purposes is a violation of this policy.
- Workers are restricted from accessing, or attempting to access, any data that has been intentionally blocked, password-protected, or locked from their viewing.
- Workers may have access to, but should not read, search for, or take, any data that is immaterial to their job role, function, or duties.
- Workers must not, or attempt to, access and browse through other workers computers or mobile devices.

Storing Confidential Data

- Ensure confidential data is always stored in the appropriate electronic and/or physical location.

22. Conducting Company Business on Personal Computers or Accounts

Personal ~~Computers~~ Devices

Employees must not use personal devices for business purposes. If accessing data via a personal computer or other device is unavoidable the personal computer or other device must have similar security controls (i.e., firewall protection, anti-virus, anti-malware, etc.) installed as those on CR-issued computers, or as deemed sufficient by the Information Security Team and/or the Company's IT Department.

Personal Accounts

While not expressly prohibited for personal use during work hours, the following must not be used for business communications:

- Social media applications, such as Facebook, X, Instagram, and LinkedIn unless authorised.
- Personal email, non-CR email, or any other communication channels that can be used for text messaging or file transfer. This includes sending business related files, emails, or messages to one's personal email.
- Personal applications and accounts used during work hours should be limited and should not interfere with an employee's job duties or breach any CR policy.

Social Media

Social Media is a critical Marketing application within the business environment and as such has grown rapidly in its importance to the business for brand awareness and to support product launch initiatives. Being able to leverage both CR's account network and workers personal networks is very important and valued. CR values the enthusiasm of its workers to share successes and stories with their networks and aims to encourage this activity. These rules are necessary to ensure this critical Marketing channel is managed in a way that removes brand and reputation risks and maximises Marketing effectiveness for the company and its products.

It is a requirement that employees and contractors representing CR are required to read and adhrere to CR's social media policy.

23. Managing Confidential Data Off-Premises

- In the event that confidential data is taken off premises, the data must be kept in a secure place and returned promptly to the Company's premises.
- Exercise caution when displaying or discussing confidential data in public places, in the presence of outside vendors, or in the presence of others (non-Company employees, the general public, etc.).
- Never leave confidential data in public spaces such as, but not limited to, conference rooms, lobbies, wastebaskets, desks, or anywhere else where the data could be seen or retrieved.

24. Deletion of Data from CR and/or Personal ICT Systems and Devices

If a CR ICT Device is lost or temporarily misplaced, this must be reported immediately to the IT Department. The IT Department will take steps to change the password of the device user and/or initiate a remote wipe of all information stored on the device.

Workers who use personal devices to connect to CR's ICT Systems are deemed by the guidelines of this policy to have consented to the CR ICT Department taking steps to remotely wipe any CR data stored in that device in the event that it is lost, or the worker ceases to work for CR. Departing workers should contact CR ICT Department to arrange for data to be removed. If the IT Department needs to remotely wipe a device without having first been contacted by the affected individual, they will take reasonable steps to only delete CR information but there is a risk that a remote wipe may also delete personal information.

25. Web Security

- IT will deploy Mimecast Web Security to all Windows clients to protect against malicious website.
- Users can request access to blocked websites by logging a service desk support call.
- Anyone who receives a warning regarding the safety of a website should stop accessing it immediately and report it to IT Services.

26. Password Management

Password Requirements

Network passwords are configured to meet the following requirements:

Password Creation

- All user and admin passwords must be at least 10 characters in length.
- Passwords should be unique, and not used for any other system, application, or personal account.
- Passwords must not contain your name.

Passwords must contain three of the following:

- Uppercase letters of A through Z
- Lowercase letters of a through z
- Digits 0 through 12
- Non-alphanumeric characters ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Default installation passwords must be changed immediately after installation is complete.

Password Protection

- Passwords must not be shared with anyone (including co-workers and supervisors), and must not be revealed or sent electronically.
- Passwords shall not be written down or physically stored anywhere in the office.

- When configuring password "hints," do not hint at the format of your password (e.g., "zip + middle name").

Enforcement

- It is the responsibility of the end user to ensure enforcement with the policies above.
- If you believe your password may have been compromised, please immediately report the incident to the IT Department for password change.

Account Lockout

Employees will be locked out of their accounts for a duration of thirty (30) minutes after five (5) consecutive, unsuccessful attempts.

Password Guidelines

- Immediately request to have your password changed by the Company's IT Department upon suspicion of compromise or if a known disclosure was made to another person.
- Do not reveal passwords to another person, including other employees at the Company.
- Do not text passwords.
- Do not use the same password for more than one account, such as personal email or social networking account passwords for Company accounts.
- Do not reveal or send a password via telephone, email, instant messaging, or other electronic communication channel.
- Do not save passwords on any automated log on tools, such as internet auto-save password options and "Remember Password" links.
- Do not write passwords down and leave in plain sight of others.
- CR's access security is managed through Multi Factor Authentication (MFA).

27. Mobile Device Management

- It is the responsibility of any CR employee using a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are applied.
- Connecting personal mobile devices to corporate and corporate-connected infrastructure is restricted.
- All mobile device purchases must be approved for purchase by the employees one-up Manager. IT will provide set up.
- Employees must report a lost or stolen mobile device to IT Department so confidential data on lost or stolen devices can be remotely wiped.

28. Software Management

Software Usage

Employees must obtain approval prior to installing any software. New software requests must be submitted through the IT Service Desk and include one-up manager approval before purchase.

The Company will monitor computers on an ad-hoc basis to ensure unauthorized software has not been installed and reserves the right to immediately remove any unauthorized software upon discovery which could result in the loss of data.

Software Restrictions

Installation of software on computing devices can introduce vulnerabilities to CR network which may result in data leakage or other cybersecurity incidents. As such, employees are prohibited from installing and using the following software to any Company computers:

- Software that automatically synchronizes files offsite (i.e., Dropbox, Google Drive, etc).

- Any gaming and/or entertainment software, including playing games over the internet.
- Software not easily identifiable by manufacturer or function.
- Unauthorised or unlicenced software.
- Any software that cannot be directly linked to that individual's role.
- In any circumstances where software is required to be downloaded it is the Employee's responsibility to first check and confirm with the IT department.

Software Development

CR IT Department have a centralised team of software developers for the purposes of continuous improvement upon the CR corporate platforms, all development is conducted within the supplier guidelines (i.e, Microsoft and others). Refer ITP-04 Solution Design, Enterprise Architecture & System Lifecycle Management V2.0.

29. Web-Based Applications

Employees are prohibited from using unapproved web-based applications that provide offsite data storage and transfer services for business purposes (i.e., dropbox.com or drive.google.com). CR data must not be transferred to and stored on such sites under any circumstance. If large data files cannot be transferred via a Company-approved method, employees must consult with the Information Security Team to establish the appropriate data share or transfer method.

30. Information Transfer

The below is applicable to any CR employee handling CR data including personal and sensitive data.

Before transferring data consider the method, nature of the information, its sensitivity, confidentiality or value and size.

Employees should be mindful that emails are not designed to attach and transfer copious amounts of data. file attachments that exceeds the total of 25MB, consider an alternative secure method of transferring sensitive data wherever possible and practicable (refer below note). All passwords must be transferred using an alternative method of communication to the recipient. Email messages must contain clear instructions of the recipient's responsibilities and instructions on what to do if they are not the correct recipient. Care must be taken as to what information is placed in the subject line of the email or in the accompanying message. Filename or subject line must not reveal the full contents of attachments or disclose any sensitive personal data. Emails must be sent from your CR provided email address to ensure the correct privacy and security information is displayed.

Note: Alternative options for secure external data transfer, outside of the standard email attachments and One-drive file sharing. These are (1) Sharefile.com and (2) Box.com – both options require one up manager approval with justification via a submitted help desk request for account creation. Terms and conditions of use available via both websites.

31. Physical Media Transfer

Removable Media Usage

The use of removable media is not permitted at CR. However, an employee can be granted permission by the IT Team if one-up manager approval has been received. This includes bringing removable media devices to and taking removable media devices out of CR offices. Use of removable media will be monitored and data managed via global policy and content visible as 'read only'.

For completeness removable media is defined as devices that can transfer data with a computer that can be plugged in and out when required. Common examples include USB, portable hardrives and company mobile phones used to transfer data.

32. Removable Media Security

It is possible to unintentionally introduce viruses that can spread to all computers on the Company's network. While virus protection software should scan removable media devices automatically, employees should transfer data from removable media devices with caution.

33. Physical Access

Access to the server rooms is limited and requires either key or swipe card access depending on the branch security and building provisions.

Employees must accompany guests at all times while they are at the Company's premises, not leave them unaccompanied and only allow access to certain rooms, areas or offices, as necessary.

For further information please refer to the site security procedure – PRO 0984.

34. Network And System Security

Security Controls

CR maintains anti-virus and anti-malware protection on all computers. The Company's network perimeter, including VPN connections, are firewall protected. Email and web content filtering tools are used to prevent against spam and phishing attacks. Email communications are encrypted and attachments are scanned for malicious code or software.

Patch Management

The Company's IT Department is responsible for ensuring the latest security patches are applied to the Company's systems and devices. Servers and Workstations are configured by Group Plolicy to check for Microsoft patches daily and automatically install. System reboots where required are scheduled betweek 6:00pm and 6:00am local time, users can defer installation of updates by up to no more than 2 device reboots.

The patch management process includes:

- Defining mandatory patch levels and determining how a required patch to the Company's systems will be identified and deployed.
- Reviewing vulnerability assessments to identify systems that may be missing required patches.
- Evaluating patches and determining deployment procedures.
- Deploying patches in a timely manner.

Vulnerability Management

The Company's IT Department is responsible for:

- Monitoring and identifying vulnerabilities – CR utilise Vulnerability management software and remediates vulnerabilities as required.
- Correcting or improving systems to prevent, minimize, or mitigate adverse system impact.

  In addition, CR performs internal vulnerability on a monthly basis and external Penetration testing annually.

35. Data Backup and Retention Policy

High Availability

All Azure virtual machines (VMs) are configured to use Managed Disks, these disks automatically manage replication of the VM disks in case of failure – 3 copies of all data Locally Redundant Storage (LRS).

Backup

Azure Backup is enabled for all live production VMs.

There are two backup policies depending on the type of server.

Reference: ITP-03 CR IT Backup Archive and DR Procedure.

Note: All Backups use Geographically Redundant Storage (GRS). Backups are stored in a separate region to the live VMs.

Microsoft Dynamics Lifecycle Services (LCS) perform the point-in-time restore (PITR) for a sandbox user acceptance testing (UAT) environment. Microsoft maintains automated backups of the business and financial reporting databases for 28 days for production environments and 7 days for sandbox environments.

36. Data Destruction

Paper Documents

A third party is contracted to provide a shredding and disposal service for CR's paper documents, invoiced monthly and collected as requested. Contract for shredding and document destruction are stored in MyOsh. Employees must place confidential documents in the designated lockbox located at the office for subsequent shredding and disposal. The third party shall confirm that proper destruction procedures were followed by providing a letter of attestation or data destruction certificate to the Company.

If confidential documents are taken outside of the Company's office, employees should shred or properly destroy the documents prior to disposal.

Equipment

Prior to the repair, redeployment, or disposal of any equipment, all confidential data stored on such equipment shall be wiped using Windows built in tools to securely erase files from drives that cannot be recovered.

Equipment can be re-purposed across the business once this process has been completed. Equipment shall not be re-purposed if this process has not been completed.

If a third party is engaged to dispose of the Company's equipment, the Company will wipe any confidential data prior to its disposal. The third party shall confirm that proper destruction procedures were followed by providing a letter of attestation or data destruction certificate to the Company. If in need of repair, the Company will choose to either wipe or encrypt the confidential data stored on the defective equipment prior to releasing it to a third party.

37. Cryptography Management

Cryptographic algorithms must meet the following criteria:

- Proven, standard and publicly reviewed cryptographic algorithms and technologies should be deployed wherever possible.
- Where proprietary cryptographic algorithms are to be deployed, they should be reviewed by qualified experts outside of the vendor in question and only deployed after approval from the Head of IT.
- Encryption algorithms or technologies should be selected in line with the information classification to be protected.
- The required level of protection is identified considering the type, strength and quality of the encryption algorithm required.

In addition, cryptography is generally required in the following scenarios:

- on mobile devices such as laptops, tablets, and smartphones;
- for authorised use of removable media such as USB memory sticks;
- where classified data is transmitted across communication lines that extend beyond the boundaries of CR, for example over the Internet; and
- where cloud services are used, regardless of the type of cloud service (for example IaaS, PaaS, SaaS).

Encryption and Digital Signature Algorithms

Industry-approved strong cryptographic algorithms with strong keys for encryption and/or digital signature should be used:

- Symmetric encryption: AES with 128-bit key (minimum) and 256-bit key (recommended);
- Asymmetric encryption: RSA with 2048-bit key (minimum) or higher, ECC with 256-bit key (minimum) or higher, Diffie-Hellman Key Exchange; and
- Digital Signature: SHA-2 or SHA-3 for hashing; DSA, RSA or ECDSA for encryption.

Encryption Key Management

CR's key management is based on the use, protection, and maintenance of cryptographic keys through their whole lifecycle. The following guidelines should be followed for managing secret keys:

- cryptographic keys will be stored securely and in the fewest possible locations;
- cryptographic keys will be securely distributed and have a data classification level of Restricted; and
- Certificates, secrets and keys will be renewed as appropriate for the platform requirement (and set as maintenance reminders in the Manage Engine Maintenance platform

Processes are to be implemented to securely retire or replace cryptographic keys. These will include key changes where the integrity of the key has been weakened due to personnel departure or keys are suspected of being compromised.

Where manual clear text key management operations are used, these operations should be managed using split knowledge, and dual control, i.e., two or three people know only their key component, which when combined, reconstruct the entire key.

Processes should be implemented to prevent unauthorised distribution of cryptographic keys.

All key custodians should formally acknowledge that they understand and accept their custodial responsibilities.

All activities associated with key management will be logged and audited to identify misuse.

Private keys should be marked as non-exportable in a Certificate Signing Request.

Storage of keys within source code or binaries shall be avoided wherever possible.

Digital Certificates

Digital certificates should be signed by a Digital Services-approved certificate authority (CA):

- Select a key size of 2048 bits or greater;
- Select an expiration of not more than two (2) years; and
- Use a new public-private key pair when the certificate is renewed. Private keys should not be re-issued or reused.

Code signing certificates should restrict access to the smallest group possible.

Self-signed certificates can only be used on protected private networks and should not be used for any production purpose on a public network.

38. Third Party Management

To ensure that CR's data and information assets are kept as secure as possible, it is necessary to assess the security posture of Third-Party Organisations (suppliers) inclusive of services provided to CR.

Contracts with Third Parties
For any engagement, a formal contract should be entered between CR and all third parties providing service to CR or using CR's information assets. Contracts should refer to all the necessary security conditions and service levels to ensure compliance with CR's security policies and standards.

- All contracts should be examined by legal counsel in conjunction with the relevant CR management where required. **Non-Disclosure Agreement (NDA)** – the third party / supplier should sign an NDA before the provision of any service to CR.
- **Data Ownership** – CR should ensure that it retains the "exclusive" right to data ownership throughout the duration of the agreement. Ownership includes all copies of data available including backup if any.
- **Data location** – CR should list the contract country(s) that are acceptable for data to be stored if applicable.
- **Legal Prevalence** – CR should ensure that the third parties own Data Privacy Policy complies with the applicable laws in Australia (or any other jurisdiction CR deems appropriate).

- **Data breach notification** – CR should contractually ensure that they are notified of any confirmed breach without any undue delay.

Service Level Agreements (SLAs) should be considered to provide both CR and the third party with the necessary checks and balances to ensure that all services provided by third parties are clearly identified considering expected levels of service, security, monitoring, contingency, and other stipulations as appropriate.

Onboarding Assessment of Third Parties

All third parties (inclusive of outsourced parties and/or contractors) should be assessed prior to any engagement.

Relationships between CR and the third party should be managed clearly through an identified point of contact/relationship manager and centralised in a registry.

All third parties should be assessed and reviewed to determine the inherent risk which could include but is not limited to:

- Confidentiality of data handled.
- Criticality of services provided by the third party to CR.
- Specific impacts to CR in the event of any incident *i.e., financial, reputational, regulatory.*
- Third party redundancy and/or replacement.

Monitoring of Third Parties

Material changes to the provision of services by third parties, including maintaining and improving existing information security policies, procedures, and controls, should be managed to involve re-assessment (if required).

Periodic reviews of the third party's services should be conducted. **Offboarding of Third Parties**

At the end of the outsourcing arrangement between CR and the third party the following actions should be taken:

- CR should arrange to promptly revoke access to all physical locations, and information assets to which the third party had been granted access.
- The third party should fully adhere to CR's requirements for returning all CR information assets, including providing evidence of the secure and permanent erasure of CR data from the third party's systems including backup.
- The third party should be obliged to reminder of all its personnel of the ongoing requirement to confidentiality and the obligations of the NDA.

39. Information Security Risk Management

Third-Party Access

CR and its third parties must agree to a written confidentiality or non-disclosure agreement prior to sharing CR confidential data. The agreement will address the third parties' duties to securely manage the Company's data and property as well as any other requirements deemed necessary by the Company. Third parties will be granted access to the Company's data on a need-to-know basis. Employee Responsibilities

Employees must:

- Escalate an unidentified third-party to the Information Security Team or ensure the third-party has a confidentiality or non-disclosure agreement with the Company prior to communicating or sending confidential data to the third-party. Refer to CR Confidentiality Agreement in MyOsh.
- Provide access to the Company's confidential data only as needed.
- Refrain from sharing or revealing, physically or electronically, any confidential data to a third-party unless authorized.

- Only send confidential data through the authorized method established by the Company, (Secure File Transfer Protocol, password-protected, encrypted, etc).

40. Consequences of a Breach of Policy

Employees who engage in activities prohibited by this policy will be subject to disciplinary action in accordance with CR disciplinary procedure, which may include termination of employment. If a contractor engages in activities prohibited by this policy, appropriate action will be taken under the relevant contract of engagement and may result in termination of the contract.

Malicious or vexatious complaints, and particularly if persistently made, may lead to disciplinary action against the complainant. Similarly, any intimidation, reprisals or victimisation against any workers raising or involved in a complaint in good faith, will not be tolerated and could lead to disciplinary action.

If through their actions or omissions workers are found to be in contravention of either this Policy or, indeed, their legal responsibility, then the company reserves the right to take legal action if it deems it to be necessary to do so. Any regulatory or legal violations may be reported to the applicable agency for civil or criminal prosecution.

CR has a legitimate interest in the private activities of workers where such activities may bring disrepute upon the company in its relationship with customers, clients, suppliers and the public and may possibly call the workers fitness for continuing employment or to provide services into question.

41. Incident Management and Reporting a Cyber Security Incident

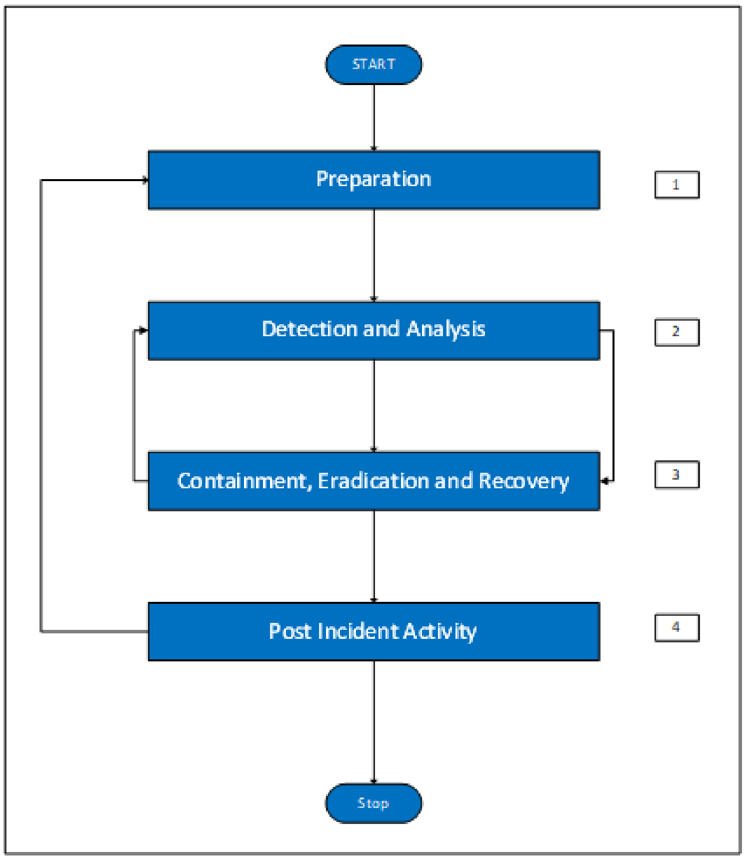
A security incident is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the company network.

All Incidences reported are treated as “High Priority” until investigated and severity determined, along with appropriate corrective actions to prevent recurrence.

Employees, who believe their computer or laptop has been compromised due to a security incident, or been improperly accessed or used, should report the situation to the IT Department’s Helpdesk selecting the **‘Priority One’** template is selected to ensure with escalation to the CR Security Officer, this will allow the source to be identified and determine the steps that should be taken to remedy the problem in accordance with the ITP-02 CR IT Cyber Security Incident Response Plan.

CR Security team members are listed in Appendix A of this Policy.

CR Cyber Security Incident Response Process Flow



42. Review of This Policy

This WISP may be amended as new developments emerge in laws, regulations, or best practice recommendations. Any changes in CR business may also require amendments to this WISP. Any material amendments will be communicated to employees. Prior to formal implementation, amendments may be issued by the Information Security Team verbally or via email. Such communications are equally valid and binding as the WISP’s written guidance.

43. APPENDIX A

INFORMATION SECURITY TEAM

Information Security Team – All member Email: infosecurityteam@crmining.com

44. ISMS Steering Committee

RESPONSIBILITY	STEERING COMMITTEE MEMBER	TITLE		
SPONSOR	Adam Zines	CFO	0458 450 004	Adam.zines@crmining.com
Business Leader	Paul Scutt	Vice President (CEO)	0476 585 913	Paul.scutt@crmining.com
	John Barbagallo	CEO		To 2nd April 2024
Human Resources	Tugce Kulac	General Manager, HR and SHEQ	0499 707 980	tugce.kulac@crmining.com
IT / Security	Karaina Morgan	Head of IT	0448 061 653	Karaina.morgan@crmining.com
CR Digital	Phil Sellers	Executive General Manager, Digital	0457 411 859	Phil.sellers@crmining.com
Product Development & Engineering	Rob Angus	GM Engineering & Strategic Projects	0434 071 811	Rob.angus@crmining.com
China	Fred Ng	GM Supply Chain	0448 007 409	Fred.ng@crmining.com
Global Digital Operations	Chris Comyns	GM Global Digital Operations	0448 497 078	Chris.comyns@crmining.com

45. APPENDIX B

DEFINITIONS

TERM	DEFINITION
Availability	Ensuring timely and reliable access to and use of data.
Confidentiality	Preserving restrictions on data so that access and disclosure is restricted to only authorized users and services.
Confidential Data	Any non-public data that could adversely affect CR if it were made available to the public.
Device	Electronic equipment controlled by a central processing unit or able to execute instructions or process data - Desktop computers, laptop computers, mobile devices, tablets, electronic notepad, servers, network devices, copy machines, printers
Equipment	Hardware (including any device or applications) leased, rented, or owned by the Company.
Incident	Any act that causes, or could potentially cause, the confidentiality, integrity, or availability of a system or the data a system processes, stores, or transmits to be compromised.
Integrity	The concern that confidential data has not been modified or deleted in an unauthorized and undetected manner.
Patch	A security fix, a bug fix, or an update which provides additional features and functions. A security fix addresses a vulnerability that may be present on a system. A bug fix corrects an error in the software code.
Removable Media	Memory and/or disk-based storage devices, such as USB drives, flash memory cards, and portable hard drives used to move data between computers.
Software	Programs, systems, or applications instructing computers to perform certain tasks. Examples may include, but are not limited to, mobile apps, gaming applications, iTunes, Adobe, Windows Media Player, Google Chrome, etc.
Suspicious Activity	Examples may include, but are not limited to, an email request from an unidentified party to initiate a wire transfer, a slow or lagging computer when prompted to open a file or document, an account password was changed without your knowledge, inability to access your account due to an unknown reason, hostile employee behaviour, etc.
System	An asset that can be defined, scoped, and managed. Examples include, but are not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices.
Third Party	An external party who has access to, processes, and stores CR confidential data. Third parties include, but are not limited to: ▪ Contractors ▪ Companies responsible for outsourced facilities or operations (i.e., IT systems, data collection services, call centre operations) ▪ Service providers (audit, legal, IT, etc.) Developers and suppliers (i.e., software products, IT systems, applications, and environments)
Vulnerability	A flaw or weakness in a system's security procedures, design, implementation, or control that could cause an incident.

46. APPENDIX C – PRO-0048 Written Information Security Policy V2.0

Approval

This authorisation is to confirm that I have received, read, reviewed, and understood the PRO-0048 Written Information Security Policy.
By signing the below, I acknowledge, agree with, and approve of the content outlined in the PRO-0048 Written Information Security Policy.

Name	Date
John Barbagallo (CEO)	To 2nd April 2024
Paul Scutt CEO	
Adam Zines	
Tugce Tulac	
Phil Sellers	
Rob Angus	
Fred Ng	
Chris Comyns	
Karaina Morgan	
Jonathan Sutherland	

Document Owner

Name:

Signed ____

Date ____

Document Approver (Head of the Steering Committee)

Name:

Signed ____

Date ____

VERSION HISTORY:

Created By		Karaina Morgan		
Date Created		23rd February 2022		
Approved By:				
Maintained By		IT		
Version Number	**Modified By**	**Date Modified**	**Approved By**	**Date**
V1.0	Karaina Morgan	23rd November 2022	ISO Project Team/ISO Steering Committee	31st March 2022
V2.0	Karaina Morgan	22/2/2023	ISO Steering Committee review and approved – Appendix C	29th March 2023
V3.0	Karaina Morgan	5/5/2023	ISO Steering Committee review and approved - minor changes	3/6/2023
V4.0	Karaina Morgan	4/12/2023	Review and sign off for ISO27001:2022 – ISO Steering Committee	8/3/2024