Information Classification, Labelling and Handling Policy

Document History & Approval

- Version control is managed by SharePoint, refer to last row in the table below.

Date	Author	Approver
2024.07.05	Melanie Nguyen, Head of Risk and Compliance	Melanie Nguyen, Head of Risk and Compliance

Document Distribution

- For the latest version of this document, please see below or contact the document author or approver:

Document Name	Location
Information Classification, Labelling and Handling Policy	The Wire – 'General Policies & Procedures' page

- Please note that printed versions of this document are considered 'uncontrolled', please refer to the above location to ensure that the latest version is being used.

Table of Contents

1. Purpose

All members of the Interactive team play a part in ensuring that our information and that of our customers, is securely collected, managed, and disposed of. This information must be protected from unauthorised disclosure, misuse, and misrepresentation, while at the same time made readily available to those who require access to that information. This policy supports the company's legal obligation to ensure that personal and sensitive information is appropriately managed and provide requirements for Interactive and third parties wishing to audit Interactive controls. This includes Interactive's compliance with applicable privacy laws.

2. Scope

This policy applies to all information collected, stored, used, processed, transmitted, or disposed of by Interactive, and outlines the responsibilities of all employees and contractors of Interactive as well as customers and third parties that Interactive share information with. This policy applies to all information assets regardless of physical or logical location, storage medium, technology used, or the purpose that it serves. Owners of information should be accountable for their classification.

3. Policy Exceptions

All exceptions to this policy must have an associated risk lodged in the risk management system. The exception must contain the business reason for the exception and the action plan to reduce the risk to within risk tolerance of the organisation.

4. Definitions

Artefact – evidence in the form of a document

Audit – inspection of a control. Refer scope for the types of audit.

Availability – Ensuring that authorised users have access to information and associated assets when required.

Confidentiality – Ensuring that information is accessible only to those authorised to have access.

Control – how a requirement is implemented. For example: a customer requirement may be that data cannot be read by unauthorised people. The related control may be role-based access controls.

Evidence – proof that a control is in place and/ or working effectively

Information Assets – Information stored in any format, e.g., document, database, system, email, etc.

Integrity – Safeguarding the accuracy and completeness of information and processing methods.

Personal Information – Information related to Interactive current employees and potential employees or customer contacts, or information that can be used to identify a person. This includes but is not limited to usernames, first name, last name, Email address, job title, location, religion, gender, marital status, postal address. Refer the below websites for the full list of applicable criteria.

https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information

https://gdpr-info.eu/issues/personal-data/#:~:text=GDPR%20Personal%20Data&text=Only%20if%20a%20processing%20of,identified%20or%20identifiable%20natural%20person.

Redact – to censor or obscure confidential information. This has the effect of reducing the classification to a less sensitive level.

Security Classification – The process of assigning value to data to label it according to its sensitivity to loss or disclosure.

5. Information Classification

All information assets shall be classified per Section 6 below.

Notes:

- Information provided by third parties that is not clearly in the public domain should receive an equivalent Interactive information classification label as detailed below.
- For customer data (i.e., data stored at Interactive as part of a service, not when customers give us information), the customer is responsible for the classification, labelling and retention of this information.

Details on how customer data is handled is in the Record of Processing Activities. Interactive's obligations for such customer data are set out in section 10.

Any disputes regarding the appropriate classification of information will be resolved by the Head of Risk and Compliance and Chief Information Security Officer.

6. Related Documents

Document	Document Location
Document Management Procedure	The Wire- General Policies & Procedures page
IT Systems Acceptable Use Policy	
Password Policy	
Record of Processing Activities	
Microsoft 365 Collaboration Overview	
Cryptography Policy	
Frontline Staff Communication Guidelines	
Flexible Working Policy	
Security Incident Response Plan	
Data Retention Policy	
Interactive Privacy Policy	https://www.interactive.com.au/privacy-policy/

7. Classifications

The table below provides detail on the classification levels of information. Interactive must adopt a 'least privilege' model when provisioning access to information. Information must only be shared on a 'needs-to-know basis' in line with the controls outlined in section 9 below.

Classification	Description & Access	Examples (Not limited to)
Highly Confidential / Most Confidential	This classification applies to highly sensitive information: i. That is protected by regulation, statutes and contractual requirements including Australian Privacy Principles and General	• Strategic business and financial plans • Firewall configurations • Network diagrams

Classification	Description & Access	Examples (Not limited to)
	Data Protection Regulation (GDPR) and the Privacy Act 1988. ii. That is related to a business unit or department operations but should not be made available outside the unit or department. iii. Whose unauthorised disclosure – may significantly adversely impact the Company, its employees, its clients and/or its partner organisations. Authorised access (to employees, contractors, and subcontractors or, for financial reports, also to customers or prospective customers) should be strictly on a least privilege basis for business-related purposes only to a specific function, group, or role.	• Any information which could create a vulnerability, such as IP addresses, cryptographic keys, etc • Information supplied by a third party that has a similar classification • Customer data (Refer to Record of Processing Activities) • Leadership Team Meeting Minutes • ELT Reports and Meeting Minutes • Personal Information Employee files • Intellectual Property
Confidential	This classification applies to sensitive information: i. That is protected by regulation, statutes and contractual requirements including Australian Privacy Principles and General Data Protection Regulation (GDPR) and the Privacy Act 1988. ii. That is related to a business unit or department operations but should not be made available outside the unit or department. iii. Whose unauthorised disclosure – may adversely impact the Company, its employees, its clients and/or its partner organisations. Authorised access (to employees, contractors, and subcontractors or, for financial reports, also to customers or prospective customers) should be on a least privilege basis for business-related purposes only to a specific function, group, or role.	• Communications with customers • Internal Audit Reports • Control testing results • Audit & Risk Assessment Reports
Internal	This classification applies to information: i. that is related to company day-to-day operations, but should not be made available outside of Interactive ii. whose unauthorised disclosure – while against policy – is not expected to seriously or adversely impact Interactive, its employees, its clients and / or its partner organisations.	• Policies • Procedures • Guidelines • Training material • Project plans • Information supplied by a third party that has a similar classification • Maintenance records • Internal audit schedule

Classification	Description & Access	Examples (Not limited to)
Commercial in Confidence / Restricted	This classification applies to information that may be shared with partners and customers who have signed non-disclosure agreements: i. whose unauthorised disclosure could seriously and adversely impact the Company, its employees, its customers and/or its partner organisations; and ii. access to which is strictly limited to a select group or process. If Commercial in Confidence/Restricted information were compromised it would cause significant damage to Interactive, and place Interactive in breach of its legal and regulatory responsibilities. Authorised access should only be available to named individuals or specified positions on a need-to-know basis for business-related purposes.	• Commercial sensitive information • Tender responses • Contracts • Information supplied by a third party that has a similar classification • hardware maintenance's configuration and firmware files that get transferred to customer's IT equipment
Public	This classification applies to information which: i. requires no special protection or rules for use; and ii. may be freely disseminated without potential harm	• Press releases • Marketing material • Public information made available via the internet

8. Legal Professional Privilege

Caveats are additional document markings that alerts readership to certain sensitivities contained therein and handling requirements. While a caveat may not alter sharing or storage requirements, they are an important tool for ensuring proper identification of sensitivities.

Caveat	Meaning
Legal-Professional-Privilege	Is a rule of law protecting communications between legal practitioners and their clients from disclosure under compulsion of court or statute. Information being transmitted to or from legal counsel, or relating to legal matters must have this marking.

9. Information Labelling Guidelines

Documents on the intranet and confidential documents sent to customers should be appropriately labelled in accordance with its level of classification. In addition, refer to the Document Management Procedure regarding format and version control requirements as applicable. Meta data can also be used to label or classify information where physical or document labels are not possible. The below label should be inserted within the footer, header or other prominent location so it can be spotted easily by those who have access to the information.

'Classification – [classification]'
For example: Classification – Highly Confidential

10. Information Handling Guidelines

Once classified, information shall be appropriately handled in accordance with its level of classification. The following table outlines minimum controls for how information should be handled in accordance with its classification.

Media	Highly Confidential / Most Confidential	Confidential	Internal	Commercial in Confidence	Public
Electronic Storage	• Must be stored in a secure location only accessible on a least privilege basis to those that require access to the information. • Should be password protected. • May be kept in off-premises (including overseas) data centres as long as the following minimum-security controls are in place: ○ Please see Cryptography Policy for approved guidelines & requirements for data protection. ○ Must be on highly available systems with approved DR and backed up	• Must be stored in a secure location only accessible on a least privilege basis to those that require access to the information. • Should be password protected. • May be kept in off-premises (including overseas) data centres as long as the following minimum-security controls are in place: ○ Please see Cryptography Policy for approved guidelines & requirements for data protection. ○ Must be on highly available systems with approved DR and backed up	• Not to be disclosed externally • May be kept in off-premises (including overseas) data centres as long as the following minimum-security controls are in place: ○ Please see Cryptography Policy for approved guidelines & requirements for data protection. ○ Must be on highly available systems with approved DR and backed up	• May be password protected as per password guidelines. • Should be password protected when shared externally • May be kept in off-premises (including overseas) data centres as long as the following minimum-security controls are in place: ○ Please see Cryptography Policy for approved guidelines & requirements for data protection. ○ Must be on highly available systems with approved DR and backed up	No restrictions

Media	Highly Confidential / Most Confidential	Confidential	Internal	Commercial in Confidence	Public
External Drives / USB	• Only to be used where there is no alternative. • External drive / USB must be first checked to ensure no other data is present. • Data must be encrypted / password protected and where this is not possible, stored in a locked cabinet when not in use. • Chain of custody logs must be maintained for any information transfer internally and externally.	• Only to be used where there is no alternative. • External drive / USB must be first checked to ensure no other data is present. • Data must be encrypted / password protected and where this is not possible, stored in a locked cabinet when not in use. • Chain of custody logs must be maintained for any information transfer internally and externally.	• Must not be used, unless specifically approved by Cyber for specific business need.	• Only to be used for the purpose of transferring specific information relating to the customer. For example, hardware maintenance transferring config files and firmware to customer's IT equipment • Nothing else should be on the drive/USB.	• Only to be used where there is no alternative. • External drives / USBs must first be checked to ensure if there are any other files on the drive, they are all classified public.
Internet applications (e.g. Search engines and AI tools)	• Highly confidential information and data must not be shared or used	• Confidential information and data must not be shared or used	• Internal information and data must not be shared or used	• Commercial in Confidence information and data must not be shared or used	No restrictions

Media	Highly Confidential / Most Confidential	Confidential	Internal	Commercial in Confidence	Public
Hard Copy	• Must be locked in a secure cabinet / draw in a locked office when unattended. • Must be transferred externally in a sealed, tamper-proof packaging and a trusted courier should be used. • Chain of custody logs must be maintained for any information transferred externally. • Clear desk policy shall be followed.	• Must be locked in a secure cabinet / draw in a locked office when unattended. • Must be transferred externally in a sealed, tamper-proof packaging and a trusted courier should be used. • Chain of custody logs must be maintained for any information transferred externally. • Clear desk policy shall be followed.	• Clear desk policy shall be followed.	• Must be locked in a secure cabinet / draw in a locked office when unattended. • Must be transferred externally in a sealed, tamper-proof packaging and a trusted courier should be used. • Clear desk policy shall be followed.	No restrictions
Data Transmission Including Email	• Must not be emailed or transmitted externally without approved encryption • Please see Cryptography Policy for approved guidelines & requirements for data protection.	• Must not be emailed or transmitted externally without approved encryption • Please see Cryptography Policy for approved guidelines & requirements for data protection.	• Must not be emailed or transmitted externally except for an Interactive (not customer) audit (see below).	• Must not be emailed or transmitted externally without signed confidentiality agreement with recipient or equivalent.	No restrictions

Media	Highly Confidential / Most Confidential	Confidential	Internal	Commercial in Confidence	Public
Video Conferencing	• Must only use the approved video conferencing application • No video recording, photography of audio recording is allowed	• Must only use the approved video conferencing application • No video recording, photography of audio recording is allowed	• Must use the approved video conferencing application or for customer audits (refer below) the customer requested application	• Must use the approved video conferencing application or the customer requested application • No video recording, photography of audio recording is allowed, without explicit consent from the disclosing party	No restrictions
Internet Social Networking	• Not to be used	• Not to be used	• Not to be used	• Not to be used	No restrictions
Facsimile	• The sending of information by fax is permitted as long as authorised persons are present both at the sending and the receiving end during the transmission.	• The sending of information by fax is permitted as long as authorised persons are present both at the sending and the receiving end during the transmission.	• Not to be used	• The sending of information by fax is permitted as long as authorised persons are present both at the sending and the receiving end during the transmission.	No restrictions

Media	Highly Confidential / Most Confidential	Confidential	Internal	Commercial in Confidence	Public
Verbal Communication	• Do not have confidential verbal conversations in public places or over insecure communication channels. Follow the Clear Desk Policy which also provides requirements around verbal communication • Voice messages left on answering services must not contain non-Public information • Begin any sensitive conversations with a disclaimer so those present know the classification level and any handling requirements of what they are about to hear.	• Do not have confidential verbal conversations in public places or over insecure communication channels. Follow the Clear Desk Policy which also provides requirements around verbal communication • Voice messages left on answering services must not contain non-Public information • Begin any sensitive conversations with a disclaimer so those present know the classification level and any handling requirements of what they are about to hear.	• Do not have confidential verbal conversations in public places or over insecure communication channels. Follow the Clear Desk Policy which also provides requirements around verbal communication • Voice messages left on answering services must not contain non-Public information • Begin any sensitive conversations with a disclaimer so those present know the classification level and any handling requirements of what they are about to hear.	• Do not have confidential verbal conversations in public places or over insecure communication channels. Follow the Clear Desk Policy which also provides requirements around verbal communication • Voice messages left on answering services must not contain non-Public information • Begin any sensitive conversations with a disclaimer so those present know the classification level and any handling requirements of what they are about to hear.	No restrictions

Media	Highly Confidential / Most Confidential	Confidential	Internal	Commercial in Confidence	Public
Any Media – for Audit Purposes	• For customer audits (i.e., audits organised by our customers): must not be shown or provided • For Interactive's audits (e.g. for ISO and SOC audits): May be provided to 3rd party auditors (NDA must be in place or with written approval from the Risk and Compliance 'R&C' Team) in the format approved by the R&C team.	• For customer audits (i.e., audits organised by our customers): must not be shown or provided • For Interactive's audits (e.g. for ISO and SOC audits): May be provided to 3rd party auditors (only with written approval from the Risk and Compliance 'R&C' Team) in the format approved by the R&C team.	• For customer audits: Can be shown to customers and/or their auditors in a closed viewing session, however any Personal Information must be redacted. • Must not be emailed or transmitted externally. • An NDA must be in place with the customer AND with their auditor. • For Interactive's audits: can be emailed or otherwise electronically transmitted to auditors, under an NDA.	• For customer audits: ○ only the information relevant to that customer's contract can be shown, emailed, or otherwise electronically transmitted. No video recording, photography of audio recording is allowed ○ An NDA must be in place with the customer AND with their auditor • For Interactive's audits (e.g. for ISO and SOC audits): May be provided to 3rd party auditors (NDA must be in place or written approval from the Risk and Compliance 'R&C' Team) in the format approved by the R&C team.	No restrictions

11. Use of couriers

- Below outlines the recommended list of couriers that can be used at Interactive.
- Chain of custody logs (i.e. consignment records) must be retained for information transfer of assets that contain non-Public information.
- Recommended Couriers:
    - Team Global Express (used in all states)
    - Activ Group:
        - DHL (used in all states)
        - Direct Couriers (used in NSW)
        - Pack and Send (used in all states)
    - Golden Messenger (used in Victoria)
    - TSS Sensitive Freight (TSS Australia)
    - Techimac (previously Computer Trans)
    - Iron Mountain
    - TIMG
    - Cope

12. Classified Government Information

- Reproduction of classified material Include must follow DSPF/PSPF Principle 10 Classification and Protection of Classified Information.
- Classifying government information assets must follow DSPF/PSPF Principle 10 Classification and Protection of Classified Information.
- For destruction of classified waste must follow Archives Act 1983 (Cth) use SCEC-approved contractors.

13. Data Retention

For data retention requirements, please refer to the Data Retention Policy.

14. Destruction Guidelines

The table below provides guidelines on how to dispose of data stored in different mediums, dependent upon the classification of the information. 'Secure bin disposal' should be with a reputable service provider who will degauss, erase and/or destroy the media as appropriate and provide a certificate of erasure and/or destruction on request. Labels and markings identifying the organization or indicating the classification, owner, system or network, should be removed prior to disposal, including reselling or donating to charity.

14.1. Media Sanistation

	Highly Confidential / Most Confidential	Confidential	Internal	Commercial in Confidence / Restricted
Hybrid hard drives - separate the non-volatile magnetic media from the circuit board containing non-volatile flash memory media and sanitise each separately.	Must	Must	Should	Must
Solid state drives and non-volatile flash memory media - overwrite with a random pattern twice to ensure that all memory blocks are overwritten[1]	Must	Must	Should	Must
Volatile media (such as RAM, which gradually loses its information when power is removed)- remove its power for at least 10 minutes[2].	Must	Must	Should	Must
Non-volatile magnetic media (hard drives, tape drives and floppy disks) - overwrite them at least once (or three times if pre-2001 or under 15 GB) in their entirety with a random pattern followed by a read back for verification.	Must	Must	Should	Must

14.2. Media that cannot be successfully sanitised

In some cases, sanitisation processes will be unsuccessful due to faulty or damaged media. In such cases, the faulty or damage media will need to be destroyed prior to its disposal.

14.3. Destroying classified information

Methods for destroying digital information include:

a. digital file shredding
b. degaussing by demagnetising magnetic media to erase recorded data
c. physical destruction of storage media through pulverisation, incineration or shredding
d. reformatting, if it can be guaranteed that the process cannot be reversed.

		Highly Confidential / Most Confidential	Confidential	Internal	Commercial in Confidence / Restricted
Paper	Archive or securely shredded or secure bin disposal	Must	Must	Must	Must

[1] Due to the use of wear levelling in non-volatile flash memory media, and the potentially for bad memory blocks, it is possible that not all memory blocks will be overwritten during sanitisation processes. For this reason, HIGHLY CONFIDENTIAL non-volatile flash memory media retains its classification following sanitisation and should be securely destroyed.

[2] Research suggests that short-term remanence effects are likely in volatile media. For example, up to minutes at normal room temperatures and up to hours in extremely cold temperatures.

		Highly Confidential / Most Confidential	Confidential	Internal	Commercial in Confidence / Restricted
		(use cross cutter if shredding)	(use cross cutter if shredding)	(can use strip or cross cutter)	(use cross cutter if shredding)
Electrostatic memory devices	Destroy using a furnace/incinerator, hammer mill, disintegrator or grinder/sander.	Must	Must	Should	Must
Magnetic floppy disks	Destroy using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.	Must	Must	Should	Must
Magnetic hard disks or tapes	Destroy using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or degausser.	Must	Must	Should	Must
Optical disks	Destroy using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or by cutting.	Must	Must	Should	Must
Semiconductor memory	Destroy using a furnace/incinerator, hammer mill or disintegrator.	Must	Must	Should	Must

Note: Media destroyed using a hammer mill, disintegrator, grinder/sander or by cutting results in media waste particles no larger than 9 mm.

Magnetic media destroyed using a degausser must have a suitable magnetic field strength and magnetic orientation.

14.4. Verification of destruction

- To verify that media is appropriately destroyed, destruction processes need to be validated with the provision of destruction certificate.

15. Destruction / De-identification of Personal Information

In accordance with the Australian Privacy Principle (APP) 11, an entity has obligations to destroy or de-identify personal information in certain circumstances, i.e. once the personal information is no longer needed for any purpose for which it may be used or disclosed. The entity must take reasonable steps to protecting, destroying or de-identifying that personal information. Further information on "reasonable steps" are outlined in the OAIC Guide to Security Personal Information.

The types of personal information collected by Interactive are outlined in Interactive's Privacy Policy.

16. Third Party and Customer Audit Requirements

During third party and customer audits, auditors and/or customers may request to view and/or be given a copy of sensitive information. We must always ensure that:

- The confidentiality and privacy of Interactive and customer data is always protected
- Customer expectations are managed and Interactive is able to deliver on those expectations

Section 9 provides guidance on what type of information can and cannot be shared during an audit. Interactive can only show / provide information with customers and auditors who have directly signed Interactive's NDA, i.e., there must be an NDA between the customer's auditor and Interactive before any information can be shown / provided to them (or where written approval have been provided by the Risk and Compliance team).

Where a customer has requested evidence of a control, Interactive may redact the source evidence to remove confidential information, in effect declassifying the information to a 'commercial in confidence' level. For example:

- For a Company policy classified as internal only, provide the version control table and table of contents only
- For a screen shot showing technical settings on a customer system, provide the screen shot redacting Interactive specific information (for example: place a black box over Interactive system names and specific employee names to make them illegible)

Where a customer has requested to confidential information about Interactive, for example: evidence of the use of a fire suppression system, it is important that no confidential documents are provided to the requestor. Instead, an on-site visit should be organised. No photos, video, audio recording or other evidence may be retained by the customer or their third party. Discretion must be used to ensure all parts of this policy are adhered to.

In addition, any Personal Information of Interactive's staff, customers or contractors must be redacted, unless absolutely necessary for the auditor to perform the audit, in which case the Head of Risk and Compliance must approve the Personal Information not being redacted.

17. Maintaining Confidentiality

Each Interactive employee is obligated to ensure the security, privacy and confidentiality of, without limitation:

a) all Personal Information and Confidential Information collected and held by Interactive, including but not limited to Personal Information and Confidential Information of Interactive, its employees, customers, and suppliers; and
b) customer data that is stored with Interactive in connection with our services.

This obligation includes, but is not limited to, the requirement of Interactive employees to protect the quality and integrity of, appropriately manage the sharing of, and to ensure the safe and secure filing of, electronic and physical copies of all Personal Information, Confidential Information, and customer data.

Interactive employees must process Personal Information, Confidential Information, and customer data in accordance with, without limitation, their employment contracts, Interactive policies, training and direction from Interactive Human Resources or management and, where applicable, the agreement for services between Interactive and the customer.