Records and Information Management Policy

Document Information

Version Number	1.0
Last Update	15/10/2022
Author	Matthew Coutts
File Name	Records and Information Management Policy
Document Title	Records and Information Management Policy
Document Owner (Role Position)	Global Head of Enterprise Technology, Risk and Cyber Security
Responsible Executive (Role Position)	Chief Technology Officer

Document Revision History

Version	Issue Date	Author	Comments	Approved By
1.0	20/10/2022	Matthew Coutts		Matthew Coutts

Document Approval and Authorisation by Senior Management

Version	Issued Date	Date Last Reviewed	Approver
1.0	20/10/2022	20/10/2022	Matthew Coutts

Section 1 - Audience

(1) This policy applies to all Company staff, contractors, work experience participants, as well as staff of controlled entities of the Company.

Section 2 - Executive Summary

(2) TEG's records, information and data provide evidence of transactions, development and administration and are a critical asset to the Company. They provide the foundation to support business activity, decision making, document rights and entitlements, make up the corporate memory, drive collaboration and communication, preserve knowledge, and provide stakeholders with transparency and accountability for Company operations.

(3) Having the capacity to strategically plan, readily identify, securely store, and manage records, information and data is essential to the efficient and effective operation of the Company.

(4) The Company is also obligated under a range of legislation to maintain appropriate records, reproduce records, or retrieve documents.

Section 3 - Purpose

(5) This policy outlines how TEG will govern the management and minimise risk relating to records, information and data and preserve assets of corporate and community significance.

Section 4 - Scope

(6) This policy applies to records, information and data in any format that is created, received, or maintained by TEG, and that documents research, deliberation, advice or actions undertaken in the course of carrying out a Company function or activity (called herein 'TEG Records').

Section 5 - Policy Specific Definitions

(7) In the context of this policy:

a) "High risk records" means those TEG records, information and data that are created in high-risk business processes or functions or received in high risk areas of the business that would be considered at a level of risk that is outside the TEG's risk appetite if they were misused, released inappropriately, or inappropriately accessed and altered, lost damaged or destroyed prematurely;
b) "High value records" means those TEG records, information and data that enable the Company to continue their functions, provide a service, and respond to audits, investigations and legal issues.
c) "Company function or activity" means any decision, action, or risk assessment undertaken by or on behalf of the Company to further its statutory objectives, including but not limited to administration, development, strategic and business planning, ensuring health and safety, client administration, consumer administration, human resource management, financial management, governance and administration of the Company, and commercial activities.
d) "TEG records" refers to physical and digital records that are created whilst performing a Company function or activity, including but not limited to paper based records; databases; emails; scanned documents; records created in collaboration sites such as (but not limited to) MS365-Teams, SharePoint, document libraries and OneDrive; completed on-line forms; actioned workflows; records created in cloud based third party applications; photos; video footage; webpages; and social media content.
e) "disposal" refers to processes and decisions associated with record and information retention, destruction or transfer which are documented in disposal authorities.

f) “records management” refers to the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including people, processes, and systems used to capture and maintain evidence of and information about business activities and transactions in the form of records.
g) “Retention period” refers to the minimum period of time for which records should be meeting regulatory, business, audit, legal and financial requirements before they can be destroyed.
h) “Information Users” refers to individuals who have been granted explicit authorisation by the relevant Information owner to access, use, alter, or destroy information within a TEG approved information system.
i) “sentencing” refers to the process of classifying records to determine how long they need to be kept and in accordance with the disposal authorities. Sentencing ordinarily takes place upon creation of a record; and
j) “Inactive records” refers to those records that are not required to meet immediate business needs, but which must be kept (in accordance with retention and disposal authorisation) to support business activities, legal or regulatory requirements, or societal expectations.

Section 6 – Principles

TEG Records and Information Management Program

(8) The program, including policies, procedures, people, and systems required to manage Company records will be monitored and evaluated for risk management, continuous improvement, and assurance that the needs of TEG, the community and regulatory requirements are met.

Ownership, control and custody of TEG Records

(9) All TEG records created or received while performing a Company function or activity are owned by the Company, unless otherwise specified under contract, and must be managed in accordance with this policy.

Creation and Management of TEG Records

(10) Information owners must:

a) assess, document and review the TEG records that will be created and captured as part of a process that they are responsible for, and determine how long these TEG records need to be kept to meet the requirements of this policy.
b) ensure that the TEG records they are responsible for are reliable, accurate, usable, stored and appropriately protected within a TEG Approved Information System or a compliant storage area (for physical records); and
c) ensure sensitive, personal, and confidential TEG records are:
    a) protected against unauthorised access.
    b) not kept for any longer than necessary; and
    c) destroyed in line with the relevant disposal authorities.

(11) Prior to entering arrangements with third party providers to store and manage TEG records, an evaluation must occur to determine and mitigate risks associated with storing TEG records outside of TEG control.

(12) Email folders, shared drives, personal drives, external storage media or unsupported cloud-based storage services (e.g., drop-box) must not be used to store TEG records as these lack the necessary record-keeping functionality to protect the records. TEG records held in these systems must be incorporated into the TEG's Approved Information System to prevent them from being inaccessible, lost, leaked, prematurely deleted or over-retained. Records with a high or medium risk rating must be stored in the approved TEG's Records Management System.

Retention and Disposal of TEG Records

(13) Retention periods for TEG records consider the needs of the business, legal and accountability requirements, and community expectations.

(14) TEG records that are inactive and no longer required to meet immediate business needs but are required to be retained until they have met the minimum retention requirements, can be moved to approved semi-active or long-term storage repositories.

(15) Destruction of TEG Records prior to completion of the minimum retention period is prohibited. Records having limited or incidental relevance can be destroyed in accordance with Normal Administrative Practice (NAP).

(16) Destruction of TEG records must be authorised, secure, timely and documented to minimise risks associated with records being accessible beyond their requirements; to reduce costs associated with record storage; and comply with Privacy Legislation.

TEG Records and Information Management Systems

(17) Information owners must consult with Records Governance Services prior to implementing new or upgrading existing TEG Approved Information Systems to ensure record management requirements and obligations can continue to be met.

(18) System Owners and System Administrators must ensure that appropriate design and maintenance documentation is developed to assist with monitoring, auditing, and ensuring records and information management systems operate as expected.

Access to TEG Records

(19) Information owners and System Administrators must ensure that TEG records for which they are responsible for are protected from unauthorised access, disclosure, modification, loss, or damage. Particular attention must be given to restricting access and securing sensitive, personal, health, and confidential records and information.

(20) Information owners must periodically review access to systems that they are responsible for to ensure information user’s access is relevant, and to remove information user’s access to systems when it is no longer required.

Security of TEG Records

(21) TEG Approved Information Systems must meet the requirements of the TEG's Information Technology Security policies, procedures, guidelines, and manuals so that TEG records are protected and available wherever they are located.

(22) Security classifications must be applied to all TEG records in accordance with the Information Security Data Classification and Handling Manual. Security classifications are based on sensitivity, risk, and potential impact on the Company in the event that the records or information is disclosed, misused, misinterpreted or lost.

(23) Physical TEG Records must be stored securely and have appropriate environmental controls in place

(24) System Owners and System Administrators must ensure the implementation of established information security policy and procedures; in the system they are responsible for. For more information, please refer to the Information Security Policy.

Out-sourcing TEG Records

(25) Information owners must assess out-sourced information systems prior to their use to ensure recordkeeping requirements and risk management requirements meet the Company’s guidelines.

Decommissioning and Migration of IT Systems and Data

(26) Decommissioning of information systems and legacy data must be planned and documented.

(27) Migration and conversion processes must be planned, documented, and tested to ensure that the Company’s records that are migrated and/or converted remain accurate, reliable, and useable, and that metadata remains associated with the records.

Risk and Business Continuity

(28) The Company will ensure its Business Continuity Plans for critical processes identify the risks to high risk records and high value records, and will implement processes to monitor and manage these risks in line with the Company's Business Continuity Management Framework. This includes, but is not limited to, appropriate back-ups and disaster recovery strategies.

(29) Information owners must determine the level of risk associated with the records that they are responsible for and apply a risk-based approach when considering the best way to manage and store records.

(30) High risk records and high value records must have more rigorous records management processes applied, whereas low risk and low value records have more flexibility in their record management provided that key recordkeeping and privacy obligations are met.

(31) Staff must plan and facilitate the transition of records to the most appropriate person or business unit to minimise disruption of operations and loss of information prior to a staff member leaving the Company, or when there is a restructure.

Monitoring

(32) Regular assessment of the effectiveness and efficiencies of recordkeeping processes is required to ensure that they support the functions and activities of the Company as well as compliance requirements.