Data Protection Policy

Data Protection Policy

Contents

Purpose

The purpose of this policy is to ensure The Connection Coach (TCC):

- Complies with data protection law and follow best practice
- Protects the rights of staff, customers, stakeholders and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

This policy also seeks to ensure the consistent application of controls to the TCC's information asset and ICT resources by establishing appropriate data classification labels. These classifications are determined by the CISO, and are based on the sensitivity of the information and the potential impact on TCC in the event that the information is disclosed, misused, misrepresented or lost.

Executive Summary

TCC routinely gathers, stores, processes, transmits and disposes of information. That information must be protected from unauthorised disclosure, misuse and misrepresentation. At the same time, it must be readily available to those who need it. The classification of information in terms of its business criticality is an essential element in achieving appropriate information security.

Scope

This policy outlines the TCC's standard data classifications, and the standard handling controls required to protect TCC information. This policy supports the TCC's legal obligation to ensure that private information is managed in accordance with the principles outlined in the Data Protection Act 2018.

Audience

This policy applies to:

- All TCC office locations
- All contracts held by TCC
- All staff and volunteers of TCC
- All contractors, suppliers and other people working on behalf of TCC

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This includes but not limited to:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers

Data Classification and Protection

This policy helps to protect TCC from some data security risks, including:

- Breaches of confidentiality.
- Failing to offer choice of opt in and opt out.
- Reputational damage and brand damage off TCC and its clients.

Data Principles

The following are the data classification principles of the TCC:

a. information is an important asset of the TCC.

b. TCC uses data classifications to define the acceptable use and handling of information.

c. data classifications consider:

   i. the broader goals of TCC, both to share and restrict access to information; and

   ii. the impacts associated with restricting access to, and the sharing of, information.

d. the user is responsible for determining the value of information within information systems and assigning an appropriate data classification label.

e. data classifications are assigned based on the information's value, legal requirements, sensitivity and criticality to TCC.

f. information within information systems is managed throughout its lifecycle:

   i. to ensure the confidentiality, integrity and availability of information; and

   ii. to achieve compliance with TCC's legal and regulatory responsibilities.

g. these principles apply to all TCC information assets stored and processed on all ICT systems and assets, regardless of physical or logical location, storage medium, technology used, or the purpose(s) they serve; and

h. any disputes regarding the appropriate data classification of information will be resolved by the TCC Director.

Data Classification

Information and assets shall be classified in terms of their value, legal requirements, sensitivity, and criticality to TCC. If information is subject to classification, it shall be classified upon its creation by the user according to the below guidelines and shall be re-classified by the user upon any significant change in content.

The following table lists the data classification guidelines:

	SEVERITY			
IMPACT TYPE	**Lowest**	<------>		**Highest**
Impact	**Insignificant to Minor**	**Moderate**	**Major**	**Severe**
Security – What competitive advantage does this information provide.	Little or no advantage.	Might provide some advantage.	Definite advantage.	Significant Advantage.
Likelihood of the competitors looking for this information.	Low or No Possibility.	Low Possibility.	Medium Possibility.	High Possibility.
If this asset or information is disclosed, stolen or lost.				
General / Provision of business operation and service.	Some localised inconvenience, but no impact to TCC. Disruption to operations with no permanent or significant effect on TCC.	Some impact on TCC's operational performance. Less impact on strategic goals in the medium term.	Significant effect on operational performance.	Achievement of operational and strategic goals in the medium term jeopardised. Existence of TCC under threat.

Compliance / Legal	Breach of legislation, contract, rule or policy that does not have any penalty or litigation impact. Breach of legislation, contract, rule or policy that may have an impact on the relationship with the third party or the legislator, but no long lasting effect. No litigation or prosecution and/or penalty. Regulatory consequence limited to standard inquiries.	Breach of legislation, contract rule or policy leading to escalated legal enquiries. Regulatory or legal consequence limited to additional questioning or review by legislator.	Breach of legislation, contract, rule or policy leading to possible legal action. Possible litigation or criminal prosecution and/or penalty. External enquiry or regulatory review and/or possible negative sanction by a regulatory body.	Breach of legislation, contract, rule or policy leading to significant and costly legal action with widespread potential impact for TCC. Litigation or criminal prosecution and/or substantial major negative sanction by a regulatory body.
Employees / WHS	No impact to employees / WHS	Continuity of employment concerns across TCC. WHS incident requiring significant medical attention. WHS event reported and investigated.	Significant Widespread damage to staff morale. WHS event causing serious injury, or negative environmental impact, and the relevant external authority notified.	Significant loss of staff WHS event causing serious permanent injury, death or environmental. Impact leading to costly action and widespread impact on TCC and/or senior staff.
Financial	$25-50k.	2-5% budget or $50k – 250K.	5-10% budget or 250K – 500K	Over 500K
Reputation	No impact to reputation.	Community concern. National media coverage and	Loss of confidence in TCC. Sustained adverse national media and public coverage.	Loss of confidence in TCC. Reputation and standing of TCC affected

		external criticism. Reputation impacted with some stakeholders.	Reputation impacted with a significant number of stakeholders. Breakdown in strategic and or business partnership.	nationally and internationally. Serious public outcry and/or international coverage. Reputation impacted with majority of key stakeholders. Significant breakdown in strategic and or business partnerships.
Service Levels	Loss of less than one day's business functions. Loss of one full day of business functions.	Loss of 1-7 days of business functions.	Loss of two weeks to two months of or business functions.	Loss of over two months of or business functions.

Roles and Responsibilities

Information Owner

The Information owner is the person responsible for the business use of the information asset. The Information owner is the authoritative head, employee, or Unit within TCC

The Information owner is given the authority to collect, create, retain, and maintain information within their assigned area of control, coupled with the responsibility to protect that information on behalf of TCC

TCC Information owner may delegate some operational responsibilities but will retain accountability.

The Information owner is required to:

a. determine the statutory requirements regarding privacy and retention.

b. assign an appropriate data classification.

c. authorise access to the information.

d. specify any additional handling controls needed to ensure the confidentiality, integrity and availability of the information.

e. communicate the control requirements to the information custodian and to users of the information.

f. develop a disaster recovery or business continuity plan for the information which identifies:

   i. any potential risks.

   ii. vital information; and

   iii. communicate this to the Information Custodian.

Information Custodian

Information Custodians are those individuals who control information assets and information systems regardless of physical or logical location, storage medium, technology used, or the purpose(s) they serve. In most cases, IT Services will act as the Information Custodian.

The Information Custodian defines information systems architecture and provides technical consulting assistance to Information owners so that information systems can be built and operated to best meet business objectives.

Information Custodians are responsible for safeguarding the information assets in their possession, including implementing access control systems to prevent inappropriate disclosure, as well as developing, documenting, and testing disaster recovery or business continuity plans.

In cases in which the information being stored is paper-based, and not electronic, the Information Custodian responsibilities will logically fall to the department gathering the information. For such systems, Information Technology or Records Governance Services (RGS) can offer guidance or provide opportunities for digitisation.

Information User

Information Users are individuals who have been granted authorisation to access, use, alter, or destroy information within an information system. An Information User will be responsible for:

a. using the information only for the purpose intended

b. complying with all controls established by TCC;

c. only destroying information in accordance with the requirements as per policy.

Responsibilities

Everyone who works for or which has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The CISO (Director) is ultimately responsible for ensuring that TCC meets its legal obligations.

The CISO is responsible for:

- Keeping all employees updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure all relative initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- TCC will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Use and Storage

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. When not required, the paper or files should be kept in a locked drawer or filing cabinet. Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer. Data printouts should be shredded and disposed of securely when no longer required.