Purpose

Explain why data classification should be done and what benefits it should bring.

The purpose of this policy is to establish a framework for classifying data based on its sensitivity, value and criticality to the organisation, so sensitive corporate and customer data can be secured appropriately.

Scope

Define the types of data that must be classified and specify who is responsible for proper data classification, protection and handling.

This policy applies to any form of data, including paper documents and digital data stored on any type of media. It applies to all of the organization's employees, as well as to third-party agents authorized to access the data.

Data Classification Procedure

Describe each data classification procedure step by step. Detail who performs each step, how data is assessed for sensitivity, what to do when data doesn't fit an established category and so on.

Example of a detailed procedure:

The Data Recipient reviews each piece of data they are responsible for and determines its overall impact level, as follows:

1. If it matches any of the predefined types of restricted information listed in Appendix A, the Data Recipient assigns it an overall impact level of 'High'.
2. If it does not match any of the predefined types in Appendix A, the Data Recipient should determine its information type and impact levels based on the guidance provided in this document. The highest of the three impact levels is the overall impact level.
3. If the information type and overall impact level still cannot be determined, the Data Recipient must work with the Data Recipient to resolve the question

The Data Recipient assigns each piece of data a classification label based on the overall impact level:

Overall impact level	**Classification label**
High	Restricted
Moderate	Confidential
Low	Public

The Data Recipient records the classification label and overall impact level for each piece of data in the official data classification table, either in a database or on paper.

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

Data Recipient apply appropriate security controls to protect each piece of data according to the classification label and overall impact level recorded in the official data classification table.

Example of a basic procedure:

Data Recipient review and assign each piece of data they own an information type based on the categories.

Data Recipient assign each piece of data a potential impact level for each of the security objectives (confidentiality, integrity, availability), using the guide in this document. The highest of the three is the overall impact level.

Data Recipient assign each piece of data a classification label based on the overall impact level:

Overall impact level	**Classification label**
High	Restricted
Moderate	Confidential
Low	Public

Data Recipient record the impact level and classification label for each piece of data in the data classification table.

Data Recipient apply information security controls to each piece of data according to its classification label and overall impact level.

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

Data Classification Guideline

Use this table to determine the overall impact level and classification label for many information assets commonly used in the organization.

Customer Personal Data			
Contains personally identifiable information (PII) collected during transactions or interactions with customers, such as names, addresses, and payment details.			
Information Types			
Personal Identifiable Information (PII)	Critical data that can identify an individual customer, including but not limited to contact information, financial data, and unique identifiers.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description	Unauthorized access could lead to identity theft, financial loss, or breach of privacy.	Accuracy and completeness of data are critical to avoid errors in customer transactions or records.	Customer service and transaction processing need timely data access; however, temporary unavailability is usually manageable.
Impact Level	High	High	Moderate
Overall Impact Level	High		
Data Classification Label	Restricted		

Transaction Records			
Records of all transactions processed, including dates, amounts, and parties involved.			
Information Types			
Transactional Data	Details about the financial transactions, which are crucial for accounting, auditing, and financial reporting.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

Impact Description	Transaction details need protection to prevent financial fraud.	It is essential to maintain the accuracy and completeness to ensure proper financial management.	Must be available for financial processing and audits but not critical for immediate operational continuity.
Impact Level	Moderate	High	Moderate
Overall Impact Level	High		
Data Classification Label	Confidential		

Market Research Analysis			
Includes aggregated data and analysis of market trends, customer preferences, and competitive landscape.			
Information Types			
Analytical Data	Insights derived from data analysis, which are used to guide business decisions and strategies.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description	Exposure could compromise competitive advantage but is less likely to result in direct financial loss.	Errors in data analysis could lead to poor business decisions.	These documents are typically used for strategic purposes and do not require immediate availability.
Impact Level	Moderate	Moderate	Low
Overall Impact Level	Moderate		
Data Classification Label	Confidential		

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

Market Research Respondent Data			
This document includes individual responses to market research surveys, often containing both qualitative and quantitative data about consumer opinions, preferences, and behaviours.			
Information Types			
Survey Responses	Detailed answers and feedback provided by survey participants, which may include demographic information, personal preferences, opinions, and sometimes sensitive personal data depending on the survey's nature.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description	Respondents often expect their responses to remain confidential, especially if sensitive or personal data is shared. Unauthorized disclosure could lead to privacy violations and damage trust in the research process.	The accuracy of the data is crucial for valid research outcomes. Any alteration or tampering with responses could skew research results and lead to incorrect market insights.	While not always needed on a day-to-day basis, the availability of this data is important for analysis and reporting purposes. Delays in availability can impact project timelines and deliverables.
Impact Level	High	High	Moderate
Overall Impact Level	High		
Data Classification Label	Restricted		

Client Contracts
Legal agreements with clients detailing the scope of work, deliverables, and commercial terms.
Information Types

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

Contractual Information	Contains sensitive information about business terms and conditions which could affect negotiations and legal standings.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description	Disclosure could negatively impact business negotiations and legal compliance.	Accuracy and non-alteration are crucial for legal enforceability.	Must be accessible for reference in ongoing client engagements and disputes.
Impact Level	High	High	Moderate
Overall Impact Level	High		
Data Classification Label	Restricted		

Client System Design/Architecture Documents			
These documents contain detailed information on the technical architecture, design decisions, system components, and interdependencies within IT infrastructure. They serve as a blueprint for the development, deployment, and maintenance of software systems and networks.			
Information Types			
Technical Specifications	Includes diagrams, design choices, software configurations, hardware specifications, and network infrastructure details that are essential for system construction and integration.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description	Disclosure of system architecture can expose vulnerabilities, making the system prone to attacks or unauthorized access.	Integrity is crucial as inaccuracies or unauthorized changes could lead to system failures, security breaches, and non-	While immediate access is not always necessary, timely availability is important for maintenance,

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

		compliance with design and security standards.	troubleshooting, and upgrades.
Impact Level	High	High	Moderate
Overall Impact Level	High		
Data Classification Label	Confidential		

System Design Documents			
Budget planning documents state the potential expenses for the following year. They include data about partners and suppliers, as well as analytical and research data.			
Information Types			
Funds Control	Funds Control documents include information about the management of the budget process, including the development of plans and use programs, budgets, and performance outputs.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description	Unauthorized disclosure of funds control information (particularly budget allocations for specific programs or program elements) can be seriously detrimental to your interests in procurement processes.	Funds control activities are not generally time-critical. An accumulation of small changes to data or deletion of small entries can result in budget shortfalls or cases of excessive obligations or disbursements.	Funds control processes are generally tolerant of delay. Typically, disruption of access to funds control information can be expected to have only a limited adverse effect on operations, assets or individuals.
Impact Level	Moderate	Moderate	Low
Overall Impact Level	Moderate		
Data Classification Label	Confidential		

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

Information Types			
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description			
Impact Level			
Overall Impact Level			
Data Classification Label			

Employee Records			
Contains personal and employment-related information about employees, such as contact details, payroll information, performance reviews, and disciplinary records.			
Information Types			
Human Resources Data	Critical for HR management, includes sensitive information that could impact an employee's privacy and the company's compliance with employment laws.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description	Protection is crucial to safeguard employee privacy and comply with GDPR and other legal requirements.	Accuracy is essential for payroll, benefits, and legal compliance.	Necessary for HR operations but typically not urgent.
Impact Level	High	High	Moderate
Overall Impact Level	High		

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

Data Classification Label	Restricted

Financial Statements			
Official records outlining the financial activities and conditions of the business, such as profit and loss statements, balance sheets, and cash flow statements.			
Information Types			
Financial Data	Essential for internal management, investors, and regulatory compliance; includes sensitive financial performance indicators.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description	Disclosure could affect the business's market position and investor relations.	Must be accurate for decision-making and compliance with financial regulations.	Regular access is necessary for operational and strategic decision-making.
Impact Level	High	High	High
Overall Impact Level	High		
Data Classification Label	Confidential		

Policy and Procedure Manuals			
Documents detailing the company's internal policies and operational procedures across various departments.			
Information Types			
Operational Guidelines	Includes protocols for day-to-day operations, ensuring consistency and compliance in business processes.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

Impact Description	Generally, these are not sensitive, though certain sections might be (e.g., security protocols).	It is important that these documents are accurate and up-to-date to prevent operational inefficiencies.	Employees need easy access to perform their roles effectively and ensure compliance.
Impact Level	Low	Moderate	High
Overall Impact Level	Moderate		
Data Classification Label	Public (with select sections possibly classified as Confidential)		

Legal Agreements and Contracts			
Legal documents including terms of service, supplier contracts, partnership agreements, and nondisclosure agreements.			
Information Types			
Legal and Contractual Information	Contains terms and conditions binding the company and its partners or clients, which are crucial for maintaining business relations and legal compliance.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description	Unauthorized disclosure could jeopardize legal standing and business relationships.	Alterations could invalidate agreements or lead to legal disputes.	Necessary for reference in negotiations and legal reviews but typically not required for daily operations.
Impact Level	High	High	Moderate
Overall Impact Level	High		
Data Classification Label	Confidential		

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

Budget Planning Documents			
Budget planning documents state the potential expenses for the following year. They include data about partners and suppliers, as well as analytical and research data.			
Information Types			
Funds Control	Funds Control documents include information about the management of the budget process, including the development of plans and use programs, budgets, and performance outputs.		
Security Objectives	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Impact Description	Unauthorized disclosure of funds control information (particularly budget allocations for specific programs or program elements) can be seriously detrimental to your interests in procurement processes.	Funds control activities are not generally time-critical. An accumulation of small changes to data or deletion of small entries can result in budget shortfalls or cases of excessive obligations or disbursements.	Funds control processes are generally tolerant of delay. Typically, disruption of access to funds control information can be expected to have only a limited adverse effect on operations, assets or individuals.
Impact Level	Moderate	Moderate	Low
Overall Impact Level	Moderate		
Data Classification Label	Confidential		

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

Impact Level Determination

Use this table to assess the potential impact to the company of a loss of the confidentiality, integrity or availability of a data asset that does not fall into any of the information types described in this document.

Security Objective	**Potential Impact**		
	Low	**Moderate**	**High**
Confidentiality. Restrict access to and disclosure of data to authorized users in order to protect personal privacy and secure proprietary information.	Unauthorised disclosure of the information is expected to have limited adverse effects on operations, organizational assets, or individuals.	Unauthorised disclosure of the information is expected to have a serious adverse effect on operations, organizational assets, or individuals.	Unauthorised disclosure of the information is expected to have a severe or catastrophic adverse effect on operations, organizational assets, or individuals.
Integrity. Guard against improper modification or destruction of data, which includes ensuring information nonrepudiation and authenticity.	Unauthorised modification or destruction of the information is expected to have a limited adverse effect on operations, assets, or individuals.	Unauthorised modification or destruction of the information is expected to have a serious adverse effect on operations, assets, or individuals.	Unauthorised modification or destruction of the information is expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.
Availability. Ensure timely and reliable access to and use of information.	Disruption of access to or use of the information or information system is expected to have a limited adverse effect on operations, assets, or individuals.	Disruption of access to or use of the information or information system is expected to have a serious adverse effect on operations, assets, or individuals.	Disruption of access to or use of the information or information system is expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

Appendix A

Describe the types of information that should automatically be classified as "Restricted" and assigned an impact level of "High." Having this list will make the data classification process easier for Data Recipient.

Types of Information that Must be Classified as "Restricted"

Authentication information

Authentication information is data used to prove the identity of an individual, system or service. Examples include:

- Passwords
- Shared secrets
- Cryptographic private keys
- Hash tables

Payment Card Information (PCI)

Payment card information is defined as a credit card number in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe

Personally Identifiable Information (PII)

PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Driver's license number
- Financial account number in combination with a security code, access code or password that would permit access to the account

Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the Data Security Officer and TSD. Policy exceptions must describe:

- The nature of the exception

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital

- A reasonable explanation for why the policy exception is required
- Any risks created by the policy exception
- Evidence of approval by all appropriate parties

Review of this document: this will be reviewed annually by the Data Security Officer.

Next review date: 5th January 2025

Court Farmhouse, Hole-in-the-Wall, HR9 7JN • 0121 31 45 374 • www.tsd.digital