UNIVERSITY OF DAR ES SALAAM

Information Assets Classification and Control Guidelines

Directorate of Information and Communication Technologies

June 2024

Guideline Approval

Document name	Information Assets Classification and Control Guidelines
Version	UDSM/ICT/IACCG V1.0_2024
Prepared by	UDSM Directorate of Information and Communication Technologies
Owned by	University of Dar es Salaam
Approved by	University Council
Date Approved	
Signature	
Signed by	

Document Information

Document Name	Information Assets Classification and Control Guidelines
Category	ICT Security Policy
Related policies	• UDSM ICT Policy • UDSM ICT Security Policy • UDSM Business Continuity and Disaster Recovery Plan • Identity and Access Management Policy Records & Information Management Policy IT Risk Management Policy
Version number	UDSM/ICT/IACCG V1_2023

Details of Version History and Authors

Version No.& Date	*Changes made from the previous version*	*Changes made by*
V1.0: 01/03/2024	*First Draft Document Submitted for Approval*	*DICT Team*

TABLE OF CONTENTS

ACRONYMS AND ABBRIVIATIONS

CCC&STC	Chief Cooperate Counsel and Secretary To Council
CD	Compact Disk
DICT	Directorate of Information and Communication Technologies
DoICT	Director of Information and Communication Technologies
ICT	Information and Communication Technologies
UDSM	University of Dar es Salaam

1. THE PURPOSE OF THE GUIDELINE AND ITS RATIONALE

This Guideline defines and provides the University of Dar es Salaam (UDSM) principles and approaches for classification of data and information systems, hereby referred to as information assets, in alignment with potential level of risks they present to UDSM business and operations. It identifies rules, procedures and responsibilities of different players in protecting information assets based on information classification and categorisation of information systems.

1.1. Scope and Constraints

The UDSM collects, stores, processes, transmits, shares and disseminates different types of data about its core business of teaching, research, consultancy and public service, as well as administrative functions. This guideline focuses on establishing categories and classifications of such data and generating information based on their level of risk to the University. By doing so, it defines the access and level of access of its data to different stakeholders within and outside the University. Therefore, the guideline affects all users of UDMS information assets, which include staff members, students, contractors, third-party entities working for or on behalf of UDSM, collaborators, government entities interacting with UDSM and the general public.

1.2. Responsible Office and Enquiries

The office responsible for the implementation of this guideline is the UDSM Directorate of Information and Communication Technologies (DoICT). All communication and inquiries about UDSM Information Assets, should be directed to DICT through the following contacts:

- Telephone - +255 (0) 222 444 666/ Ext
- Mobile - +255 (0) 745 222 333 /
- Email - dict@udsm.ac.tz
- Physical Address - Office No 102, Ground floor, Cranford Pratt Building

2. THE GUIDELINES

2.1. Guideline Summary

The value of data at UDSM increases when such data is appropriately used and needed by customers. Alternatively, when data is misused, misinterpreted, or its access is unnecessarily restricted, its value decreases. Thus, this guideline is meant to provide an acceptable approach for identifying types of UDSM information assets, establishing their sources and classifying them into risk levels to facilitate the determination of access authorisation and appropriate security control. The requirement to safeguard information assets must align with the need to support the pursuit of UDSM business, functions and strategic goals.

2.2. Definitions of key terms and concepts in this guideline

i. **Data:** refers to the representation of information in a formalised manner suitable for communication, interpretation, or processing by humans or by electronic systems. Examples of data may include documents, emails, transcripts, images, audio, or video stored electronically, databases, logs, or journals.

ii. **Data Owner:** refers to a designated role within an organization who is responsible for the classification, management, authorisation and protection of specific sets of data.

iii. **Information assets:** refers to any data relevant to the University's business function stored in any manner that has some value either to the University or an individual university employee such that if it is lost or becomes inaccessible, or inaccurate, it would be difficult to replace without cost, skill, time or resource. Information assets:

   a. have recognisable and manageable value, risk, content and lifecycles.
   b. could come in any media form, such as paper, or electronic format (External Hard Disk, CDs, USBs, Hard Disk Drives, etc.);
   c. could be structured (databases, etc.) or unstructured (emails, reports, etc.);
   d. includes tangible assets (physical items) such as hardware, firmware, computing platform, network device, or other technology component; and intangible assets such as data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation.
   e. value is determined by stakeholders in consideration of loss concerns across the entire system life cycle, such as business or mission concerns.

iv. **Data Availability**: refers to methods for ensuring that required data is always accessible when needed, in accordance with university retention policy.

v. **Data Confidentiality**: refers to methods for ensuring that access to sensitive data is limited to authorized individuals.

vi. **Data Integrity**: refers to methods for ensuring that data is complete, accurate, consistent and safeguarded from unauthorized modification.

vii. **Data Classification:** refers to the taxonomy of organising data into categories, so that data may be used and protected efficiently.

viii. **Classification based on level of sensitivity:**

a. **Public Data:** This is important data that is openly shared to the public because it has the lowest level of risk and its public nature makes it unnecessary to protect its use by unauthorized individuals. *It presents no risk.*
b. **Private Data:** This should not be available for public access and should be protected through traditional security measures such as passwords. *It presents low risk.*
c. **Internal Data:** This is limited to UDSM employees and can have different security requirements dictating who can access it and how it can be used. *It presents low risk.*
d. **Restricted Data:** This is accessed by a limited number of people in the University after obtaining proper authorisation from the Data Owner or Data Custodians. *It presents medium risk.*
e. **Confidential Data:** This is the most sensitive data for the University and requires additional protection through encryption. Its access is strictly controlled to prevent unauthorized use. *It presents High Risk.*

ix. **Personally Identifiable Information (PII):** This is the information that can be used to distinguish or trace the identity of an individual, such as name, national identification number, check number, biometric records, student's registration number and driving licence number.

- PII can be used alone, or when linked with other personal or identifying information for a specific individual such as a parent's name, date of birth and place of birth.

x. **UDSM institutional data:** This refers to data owned by or in the custody of the University of Dar es Salaam.

xi. **UDSM Data Owner:** is the UDSM Vice Chancellor as the Institution Chief Accounting Officer and the Chairperson of the UDSM ICT Steering Committee, or any other UDSM employees with leadership responsibilities designed by the Vice Chancellor (designees).

a. Designees should have planning, policy-level and management responsibility for data within their designated functional units. Such designees may include Deputy Vice Chancellors, College Principals, School Deans, Institute Directors, Directors of UDSM Administration Units and Heads of Departments or Sections.

b. Designees of data custodianship can also be Coordinators/Leaders of consultancy projects or principal investigators of research projects that are registered as per the UDSM Research and Consultancy Policy.

xii. **UDSM Data Steward:** These are UDSM officials/employees with management/leadership responsibilities that make them responsible for managing one or more types of information/data. UDSM Data Steward may also be Coordinators/Leaders of consultancy projects or Principal Investigators of research projects which are registered as per the research and consultancy policy.

xiii. **UDSM Data Custodians**: These are UDSM employees or designated third-party agents, working for or on behalf of UDSM, responsible for the operation and management of information systems which collect, manage, process, or provide access to UDSM Data. The Data custodian must be authorized by the appropriate Data Steward as per the UDMS following procedures in the related UDSM ICT Management Instrument.

xiv. **UDSM Data Consumers:** These are UDSM staff members or third-party agents who works for or on-behalf of UDSM and have been granted access to UDSM information/data to enable them to perform assigned responsibilities or routine UDM functions. They are granted access to information/data by relevant authorities exclusively for the interests, business and functions of UDSM.

2.3. Roles and Responsibilities

Table 1: Data/Information Roles and Responsibilities of UDSM Members and Stakeholders

S/n	Roles	Role Holder	Role responsibilities
1	UDSM Vice Chancellor	Data Owner	i. Assigning and overseeing data custodians. ii. Overseeing the establishment of UDSM information asset policies. iii. Determining statutory, regulatory and other requirements for UDSM information assets. iv. Promoting data quality and appropriate use.
2	• Vice Chancellor • Deputy Vice Chancellors • Principals, • Deans • Directors • Managers • Head of Departments	Data Steward	i. Assigning and overseeing data keepers: individuals responsible for custodianship of specific types of data based on their roles ii. The application of this and related policies and procedures to the systems, data and other information resources under their care or control. iii. Assigning data classification levels in accordance with this guideline and associated procedures. iv. Communicating and providing education on data safeguarding to authorised users v. Authorising access, both logical and physical, only to authorised individuals who have a business need to access specific data or other information assets as per the relevant UDSM policies and regulations. vi. Authorising remote access to information assets to only authorised individuals who have a business need to access them through a secured system approved by DoICT as per the relevant UDSM policies and regulations. vii. When a particular information or dataset is maintained by more than one Data Custodians, they should work together on matters related that information/data under the coordination of DoICT to ensure data consistency and integrity.
3	• Managers • Department Heads	Data custodian	i. Ensure Information Security Controls relevant to the information/data classification level and other information assets under their custody.

S/n	Roles	Role Holder	Role responsibilities
	• Section Heads • Project leaders • Principal Investigators		ii. Ensure compliance with the UDSM acceptable use and computer security policies, standards and procedures. iii. Managing access to information, assisted by Data Consumer as authorised by the respective Data Steward. iv. Adhering to information/data handling and protection policies and procedures established by Data Owner.
4	• UDSM Staff • UDSM Students • UDSM Contractors • UDSM Clients	Data customers	i. Complying with the policies and procedures established by the appropriate UDSM Data Custodians and UDSM Data Keeper. ii. Complying with national ICT policies, eGovernment legal and regulatory provisions, laws of the land and UDSM ICT policies and regulations related to information/data and the use of information systems. iii. Implementing safeguards for protecting data as prescribed by the appropriate Data Custodian. iv. Notifying any unauthorised access or data misuse to relevant authorities: UDSM DoICT, UDSM Information/ Data Owner, relevant UDSM Information/ Data Custodian, or UDSM Information/ Data Keeper.
5	UDSM CoICT	Chief Information Security Officer	i. The UDSM DoICT is responsible for developing policies and procedures to secure UDSM information assets. ii. Such policies and procedures must be developed in line with relevant national laws and regulations as provided by the e-Government Authority and institutional policies as in the UDSM ICT management instruments. iii. Policies and procedures related to UDSM information assets have to be approved by the UDSM ICT Steering Committee prior to being operationalised.

3. INFORMATION/ DATA CLASSIFICATION

3.1. Types of UDSM Data

The University has different types of information assets. Examples of such assets include databases of various datasets; student records; examination records; data files; contracts and agreements between UDSM and its staff members, contractors, collaborators, tenants and students; policies, guidelines, rules and regulations documents; documentation of various ICT systems and infrastructure; teaching materials; training materials; operational/support procedures; risk management plans; risk registers; business continuity plans; backup plans; financial information; medical records; insurance information; human resource management records; reference material; audit trails, archived information; and emails.

The UDSM Data Steward must classify all University data into risk levels to provide the basis for understanding and applying the appropriate level of security controls. These classification levels consider existing laws, regulations, policies, contractual agreements, ethical considerations and intellectual property rights. Data can also be classified based on specific reasons that are meant to avoid the possibility of harming the University, its units, or individuals

Table 2: UDSM Data Classifications

S/n	Classification	Data type	Category	Risk level
1	**Student records** *(These include student indefinable data)*	• bio data	Confidential data	High risk
		• academic/examination records		
		• fees related records		
		• registration records		
		• change of study status		
		• accommodation records		
		• student family records		
		• sponsorship records		
		• staff and student evaluation forms		
		• coursework assessment		
2	**Financial and accounting records**	• revenue collections	Restricted Data	High risk
		• expenditure records		
		• imprest requests		
		• imprest retirements		
		• auditing reports		
		• financial reports		
		• responsibility allowances		
		• salaries and remunerations		
		• procurement bills and invoices		
		• payment records		
		• budget plans		
		• bank records		

S/n	Classification	Data type	Category	Risk level
		• Research funding agreement		
		• Research budget		
3	**Administrative** *(These include data related to day-to-day administrative functions of the university)*	• Meeting records	Restricted data	Medium Risk
		• Internal memos		
		• E-mail communications		
		• Letters		
		• Service delivery reports		
		• Clients' and staff complaints		
		• Alumni records		
		• Spreadsheets		
4	**Institutional Documents**	• Internal policies/ plan	Private Data	Low Risk
		• Rules and regulations		
		• Circulars		
		• Strategies		
5	**Human Resources**	• Staff records	Confidential data	High Risk
		• Staff appraisal records		
		• Payroll		
		• Staff disciplinary letters and reports		
6	**Research**	• Research publications	Public data	No impact
		• Postgraduate research records		
		• Research project records		
		Dissertations and theses	Restricted data	Medium Risk
7	**Consultancy** *(All information related to consultancy services provided by units and individual staff)*	• Consultancy contracts	Private data	Medium Risk
		• Consultancy reports		
		• Consultancy budget		
8	**Teaching and Learning**	• Course materials	Private data	Low Risk
		• Timetable		
		• Final year project reports		
		• Final year project records		
		• Practical training records		
		• Online teaching material		
		• Online tutorials		
		• Video and audio		
		• Powerpoint slides and hand-outs		
9	**Published documents** *(These include all documents that are made available or accessible to the public)*	• Policies	Public data	No Impact
		• Approved reports		
		• Strategic documents		
		• Statistics		
		• Website contents		
		• Social media contents		

S/n	Classification	Data type	Category	Risk level
		• Scholarship information		
		• Prospectus		
		• Almanac		
		• Service and product information		
		• New releases		
		• Market information		
10	**Library** *(These include all information made available online)*	• Library website	Low risk	Low risk
		• Digital libraries		
		• Books		
		• Membership records		
		• Scholarly materials		
11	**Health and medical records**	• Patient records	Confidential data	High risk
		• Health insurance records		
12	**Contracts, agreements and IPR**	• Memorandum of understanding	Confidential data	High risk
		• Service level agreements		
		• Service contracts		
		• Unpublished patents		
		• Staff contracts		
		• Customers records		
13	**Communication**	• E-mails communication	Restricted Data	Medium Risk
		• Office telephones		
		• E-Office correspondences		
		• Mobile phone communication		
		• text messages		
14	**Real Estate Management**	• digitised infrastructure maps and drawings	Restricted Data	Medium Risk
		• Housing allocation records		
		• House renting contracts		
		• Structure designs		
		• Title deeds		
		• Lease agreements		
15	**ICT services**	• Systems usage information	Confidential data	High risk
		• Information systems logs		
		• Configuration records		
		• Passwords to critical systems		
		• Server configuration information		
		• System monitoring information		
		• CCTV camera surveillance records		
		• Backups and recovery system		
		• Physical inventory		
16	**Information of others**	• Client's identifiable information	Confidential data	High Risk
		• Intellectual property rights		
		• Trade secrets		

3.2. Data Classification Levels

The classification level assigned to data will guide the Data Owner, Data Steward, Data Custodians and Project Teams in ways to ensure security protections and access authorisation mechanisms are appropriate for that data. The following risk levels will be used to classify UDSM data:

i. **No Impact (Green):** A data category is classified as having no impact if the loss of confidentiality, privacy or availability of the data has no impact on the University as an organisation, its members, or its clients. Such data is mainly produced for publication to allow access by the public, so it MUST NOT be protected.

ii. **Low Risk (Yellow/ Gold):** Data is classified as Low Risk if the loss of confidentiality, integrity, or availability of the data would have minimal strategic, compliance, operational, financial, or reputational risk to the UDSM, its members and its clients. This data MUST be protected and its use or release must be authorised by the relevant Data Custodian or Steward.

iii. **Medium Risk (Orange/Amber):** UDSM data is classified as Medium Risk if the loss of confidentiality, integrity, or availability, it would have moderate strategic, compliance, operational, financial, or reputational risk to the UDSM, its members and its clients. The integrity and availability of medium risk data MUST be protected and appropriate measures should be put in place to protect its privacy and confidentiality. Data access to medium-risk data must be provided to individuals who need it to enable them execute their job responsibilities and access MUST be authorised by the Data Owner or Data Steward with direct responsibility for the data in question.

iv. **High Risk (or Red):** Data is classified as high-risk (the most sensitive/critical classification) if the loss of confidentiality, integrity, or availability of the data would have a high strategic, compliance, operational, financial, or reputational risk to the University. Privacy, confidentiality, integrity and availability of these data are important and MUST be protected and access MUST be controlled from creation to destruction. Access to high-risk data MUST be requested from and authorised by, the Data Owner or Data Steward who is responsible for the data and such access shall be granted ONLY to UDSM employees who require such access to enable them to perform their job responsibilities. Also, access may be granted to individuals permitted by law in execution of legal requirements. Although the confidentiality of these data is of primary importance, their integrity MUST also be ensured. The Data Owner, after consulting the UDSM Chief Cooperate Counsel and Secretary to Council (CCC&SC) and DoICT, has the authority to classify or declassify any UDSM data as High-Risk.

4. IMPLEMENTATION, REVIEWS AND ENFORCEMENT

4.1. Implementation and Reviews

i. This guideline shall come into operation once approved by the UDSM ICT Steering Committee, and then shall be considered mandatory reference for all UDSM information assets.

ii. At all times, DoICT will ensure the classification of information assets presented in this guideline in deciding control and security measures required to control and protect UDSM information assets.

iii. This document shall be reviewed after every three years or anytime whenever the UDSM information assets change.

4.2. Roles and Responsibilities

i. It is the responsibility of the UDSM Data Owner, Data Stewards, Data Custodian, Data Customers and the Chief Information Security Officer to read, understand and implement this guideline.

ii. Users of this guideline are expected to exercise reasonable judgement in interpreting these guidelines and in making decisions about the classifications and control of UDSM information assets.

iii. Any person with questions regarding the application or meaning of any part of this guideline shall seek clarification from DICT office.

iv. The Vice Chancellor through DoICT shall enforce compliance by making sure the Data Owner, Data Stewards, Data Custodians and Data Customers understand the provision of this guidelines and implement them.

4.3. Monitoring and Evaluation

i. The UDSM ICT Steering Committee shall, in its scheduled meetings, review the classification of UDSM Information Assets and Control guideline to ensure its appropriateness to the nature of UDSM information assets.

ii. DoICT shall conduct regular assessments of the classification of UDSM information assets and establish the need for improvement and accommodating new requirements in response to the new development of UDSM information assets.

4.4. Exceptions

In case of any exceptions to this guideline, it shall be thoroughly documented and follow through a proper channel of authorisation using the same authority which approved this document.