STANDARD OPERATING PROCEDURE (SOP)		
TITLE: SOP FOR BACKING UP DATABASES, DOCUMENTS AND SYSTEMS		KNUST KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

<u>DO NOT USE THIS SOP IN PRINTED FORM WITHOUT FIRST CHECKING IT IS THE LATEST VERSION.</u>

Document ID:	*SOP-UITS-02*
Version No:	1.0
Date Authorized:	*Date_to_be_authorised*
Effective Date:	*Date_to_be_effected*
Review Date:	*three-years_after_approval*
Applicable:	Systems and Data Management Division (SDMD),UITS Information Security and Technology Assurance Division (ISATD), UITS

Author(s):	**Mr. Phanuel Seli K. Asense**
Approved by:	**Mr. Emmanuel N.O. Afful**
Signature:	*to_be_digitally_signed*
Date Approved:	

1. **PURPOSE**

   The purpose of this SOP is to document the procedure for backing up electronic databases, documents and systems of Kwame Nkrumah University of Science & Technology (KNUST).

2. **SCOPE**

   This SOP encompasses the backing up of all electronic databases, documents and systems of Kwame Nkrumah University of Science & Technology (KNUST)

3. **APPLICABILITY**

   This SOP applies to designated staff of Systems and Data Management Division (SDMD) and Information Security and Technology Assurance Division (ISATD) *of UITS, KNUST who are to ensure the electronic databases, documents and systems are backed up and secure.*

4. **TERMS**

   Recovery Time Objective (RTO: it is the maximum acceptable length of time required for an organization to recover lost data and get back up and running for each database, documents and/or system to be backed up. Given in time.

   Recovery Point Objective (RPO): is the maximum allowable period between the time of data loss and the last useful backup of a known good state or the maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organization.

5. **PROCEDURE**

Determine what data has to be backed up

1. Identify all databases, sets of documents and/or systems that needs to be backed up.
2. Determine the Recovery Time Objective (RTO), which is the maximum acceptable length of time required for an organization to recover lost data and get back up and running for each database, documents and/or system to be backed up.
   [Recovery Time Objective (RTO) is the maximum acceptable time that an application, computer, network, or system can be down after an unexpected disaster, failure, or comparable event takes place]

3. Categorize the databases, sets of documents and/or systems as :
   - *Existentially-critical* for the business to survive (High)
   - *Mission-critical* for the organization to operate Medium)
   - *Optimal-for-performance* for the organization to thrive (Low)

   Use the ISTAD's criteria for determining critical systems in conjunction with the RTO.
4. Define and layer the level of protection accordingly i.e. High, Medium and low.

Determine how often data has to be backed up

1. Determine KNUST's Recovery Point Objective (RPO), which is defined as the maximum allowable period between the time of data loss and the last useful backup of a known good state or the maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organization for each databases and documents.

2. Define the frequency with which you back up data which should be aligned with the Recovery Point Objective (RPO) of each database, sets of document and/or system. There should be a frequency for each type of backup -i.e. full backup, differential backup and incremental backup.

   NB. Rule of thumb, backups should be performed at least once every 24 hours to meet acceptable standards.

Identify and implement a suitable backup and recovery solution

1. Identify suitable backup solution for each database, sets of document and/or system i.e. the type of backup (i.e., full backup, differential backup and incremental backup), and where the data is backed up (i.e., Physical/Local backup - external hard drive, USB drive, NAS etc. or Cloud/Remote backup - off-site)

Test and monitor your backup system

1. Test backup scripts (automated, manual types) periodically to ensure they are working properly. Scheduled officers must ascertain this and report at least once a month.
2. Test backup files by restoring to ensure the process is smooth and accurate. Scheduled officers must ascertain this and report. This must be relative to the Recovery Point Objective (RPO) of respective databases, sets of documents and systems.
3. Monitor your backup performance and regularly check the logs for data lapses. Scheduled officers must ascertain this and report.

6. **APPENDIX**

Template for backup procedure (Reference log)

#	Item Name	Type (Database/Document/System)	Recovery Time Objective (RTO) -Time	Recovery Point Objective (RPO) -Time	Frequency of Full Backup	Frequency of differential and/or incremental Backup	Category: Existentially-critical (High), Mission-critical (Medium), Optimal-for-performance (Low)	Protection level: High, Medium, Low	Data location : Site – Machine – Directory (Folder)

A reporting template for Backup Officers

#	Item Name	Back up type (Full / Differential / Incremental)	Expected Date for backup	Backup Execution Date	Backup file Name	Backup File location	Process Inspected by	Remarks

SOP-UD-01	Version 1.0	4

Based on Template SOP-UD-01 Date_of_Approval_2023

Uncontrolled when downloaded or printed. Please ensure you are working from the current version.

A reporting template for Backup File Testing Officers

#	Backup file Name	Backup File location	Expected Date for testing	Backup file testing Date	Process executed by	Remarks

A reporting template for Backup Performance and Logs check Officers

#	Server Name	Back up performance remarks	Backup log check remark	Expected Inspection Date	Inspection Date	Backup performance and log check Inspected by

A reporting template for Backup Script Testing Officers

#	Backup script name	Expected Date for testing	Date tested	Remarks	Backup Script Inspected by

7. **RELATED DOCUMENTS**

   ISTAD's criteria for determining critical systems

SOP-UD-01	Version 1.0		5

Based on Template SOP-UD-01 Date_of_Approval_2023

Uncontrolled when downloaded or printed. Please ensure you are working from the current version.

8. <u>VERSION CONTROL</u>

Document History	
Version	**Summary of Changes**
1.0	N/A First issue