



INTER-OFFICE MEMORANDUM

TO : ALL EMPLOYEES ASSIGNED TO CORPORATE IT – SYSDEV
SUBJECT : RULES AND REGULATIONS
DATE : October 25, 2024

In alignment with the IT Sysdev Team Rules and Regulations, all members of our department must adhere to the approved guidelines to ensure optimal performance across each team. Furthermore, any employee who fails to comply with these Rules and Regulations may face disciplinary action for **INSUBORDINATION**.

The following teams are subject to these Rules and Regulations:

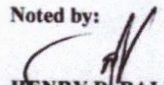
1. Programmers
2. System Analysts
3. Record Management System Team (RMS)

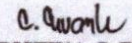
Reviewed by:


JENEFFER C. OUTANDA
IT Sysdev- Section Head


MARK ANTHONY S. RABACA
IT Sysdev- Section Head

Noted by:


HENRY D. BALIAR
Corporate IT Manager


MARIA CRISTINA C. EVARLE
IT Sysdev- Jr. Supervisor

Approved by:


MARIA NELIZA U. FUERTES, CPA, CIA, CSCU, CISA, REB, REA, CICA, CRFA, REC
Corporate Audit Group Managing Director

TECH TACTICANS

RULES AND REGULATIONS (Records Management System)

1. DOCUMENTATION AND METADATA MANAGEMENT

- **Document Metadata:** RMS personnel should ensure that each record is accompanied by essential metadata, such as creation or receive date, author (BU), and subjects (Document Type).
- **Consistency in Naming Conventions:** Use a standardized naming convention across all records folders for consistency, facilitating easier retrieval and minimizing errors.
- **Monitoring of Documents:** RMS personnel should ensure that each document, upon receiving or releasing it, is recorded in the monitoring of documents manual and digital for accountability measures.

2. RECORD LIFECYCLE MANAGEMENT

- **Creation and Capture:** RMS personnel should define processes for capturing records at the point of creation, including metadata tagging, classification, and indexing.
- **Classification and Indexing:** RMS personnel should organize and categorize data, documents, or records into distinct groups or categories based on their content, purpose, or other relevant attributes. Indexing every category of documents for efficient retrieval and organized records.
- **Storage and Retention:** RMS personnel should store records securely in formats that ensure long-term accessibility, readability, and integrity. Assign retention schedules to each document type.
- **Archiving:** RMS personnel ensure that important information is properly preserved, accessible, and protected over time, even after it is no longer needed for day-to-day operations. Storing and preserving records, documents, or data that are no longer actively used but are retained for long-term reference, legal, or historical purposes.
- **Destruction or Deletion:** RMS personnel should implement secure and documented destruction protocols, ensuring that records are only disposed of after fulfilling retention periods with proper authorization and approval.

3. SECURITY AND ACCESS CONTROL

- **Confidentiality:** Only RMS personnel are authorized to access or modify classified documents within the system without restrictions. If requested by users, users should request via RFS (Request for Setup) / TOR (Transaction Override Request).
- **Document Watermarking:** RMS personnel should apply watermarks to sensitive documents to help deter unauthorized sharing and track leaks.
- **Physical Security:** RMS personnel should ensure all physical documents are stored in secure locations such as cabinets and implement security measures like surveillance cameras and controlled entry points in areas where confidential documents are stored.

4. RECORDS TRANSFER AND MIGRATION

- **Records Transfer:** RMS personnel should ensure that every physical copy of documents transferred is recorded in the monitoring of files together with the names of the person receiving the transferred documents with signature and date returned/transferred.
- **Audit Trail for Migration:** RMS personnel should document all steps taken during migration, ensuring transparency and traceability in the process.

5. USER TRAINING AND AWARENESS

- **User Training:** RMS personnel should provide training to new users requesting access to RMS together with approved RFS (Request for Setup) and Training Attendance Sheet.

6. BACKUP AND DISASTER RECOVERY

- **Disaster Recovery Plan:** RMS personnel should ensure that all scanned documents have external backups aside from internal backups.
- **Offsite Backups:** RMS personnel should ensure that all uploaded and scanned documents are backed up in the Offsite Server Backup.


7. RECORDS ACCESSIBILITY AND RETRIEVAL


- **Search Capabilities:** RMS personnel should implement proper search functionalities within the RMS, allowing users to quickly retrieve records based on the keywords, metadata, or classification.
- **Accessibility:** RMS personnel should ensure records are accessible or tagged to all authorized personnel at any time, regardless of their location. In adding access or tagging records to users, users should request via TOR (Transaction Override Request) with approval before executing.
- **Response Time:** RMS personnel should be on time in responding to user's requests for access, tagging, and other record requests.

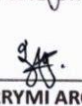
8. HANDLING SENSITIVE AND CLASSIFIED INFORMATION

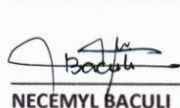
- **Data Sensitivity:** RMS personnel should define and classify records based on their sensitivity level (e.g. confidential, classified, public)
- **Document Watermarking:** RMS personnel should apply watermarks to sensitive documents, especially in uploaded records accessed by the RMS users and printouts.

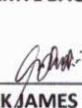
RMS TEAM:


MARK ANTHONY RABACA


FELIX DAG-UM JR


ZHERRYMI ARCAMO

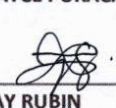

NECEMYL BACULI


MARK JAMES BITALAS


EDMUND DAJAO


ANGÉLICA CALIMBO


KAYCE PURACAN


JAY RUBIN


JOHN RYAN YAÑEZ