IT Operations Policy

DOCUMENT CONTROL

DOCUMENT NAME	IT Operations Policy
ABSTRACT	IT Policy applicable to all IT operations at Ashoka University
Owner	IT Department, Ashoka University
Co-owners	
Distribution List	Staff of Ashoka University and IFRE
Linked (Related) docs	Ashoka University Mass email and Anti-Spam Policy.

DOCUMENT INFORMATION

VERSION	REMARKS
1.0	Effective From: July 01, 2017
2.0	Effective From: July 01, 2021
Approved By	Registrar, Ashoka University

IT Policy may be amended or augmented from time to time to reflect changes in emailing and other IT services provided by the University. For any clarifications, please write to: systems@ashoka.edu.in

Any such change(s) shall be intimated to the faculty and staff by appropriate electronic communication.

TABLE OF CONTENTS

1. Scope
2. Statement & Purpose
3. Data Backup & Recovery
    a. Schedule of Backups
    b. Storage of Backups
4. Critical IT Incident Management
    a. Line of Responsibility
    b. Compliance & Monitoring
    c. Review
5. Enterprise Resource Planning
    a. Scope & Overview
    b. Maintenance, Testing & Deployment
    c. User Access Management
6. Change Management Controls
7. Policy Review

IT Operations Policy

Scope

This policy applies to all IT staff, vendors and consultants who manage IT operations at Ashoka University. This includes development and maintenance of IT systems, networks, as well as IT facilities provided by individual centers, departments, and university laboratories, if any.

Statement & Purpose

The purpose of this policy is to effectively administer and run IT operations and Ashoka and establish a safe and secure university environment.

This policy is intended to describe the following aspects of IT operations:

- Data Backup and Recovery
- Critical IT Incident Management
- Enterprise Resource Planning

This policy is established to promote a safe university environment and to ensure that the university fulfills its legal and external sponsor obligations.

Data Backup and Recovery

This section underlines the backup guideline for systems within the University. These systems typically include, but are not limited to, laptops, desktops, servers etc.

The process is designed to protect University's data and to be sure that it is not lost and can be recovered in the event of an equipment failure, intentional/unintentional destruction and/or disaster.

This applies to all equipment and data owned and operated in and by the university.

- Users are expected to ensure the safety of the data stored physically on their laptop/desktop/external drives. The IT team will provide all the assistance required for this purpose.
- For the safety of very critical data:
    - Department heads can request IT support to create a folder for the department on the server that is backed up regularly. The files on this server drive will be made accessible to the users of the department authorized by the HOD.
    - Users are advised to maintain backup of their critical data either on external media, or on Google Drive.
- **Schedule for Backups**

  Full backups are performed on the nights of Monday, Tuesday, Wednesday, Thursday, and Friday of the week. If due to any reason backups are not performed on Friday, it shall be done on Saturday or Sunday.
- **Storage of Data Backups**

  There are a separate set of tapes for each day backup and a separate set of tapes for each Friday

of the month.

Backups performed on Friday or weekends shall be kept for one month and used again in the next month on the applicable Friday. Backups performed Monday through Thursday are kept for one week and used again the following appropriate day of the week.

- **Tape Drive Cleaning**: Tape drives are cleaned weekly, and the cleaning tape is changed monthly.
- **Monthly Backups:** Every month a monthly backup tape is made using the oldest available backup tape or tape set from the tape sets.
- **Age of tapes:** The date of each tape is recorded on the tape from the date it is put in service. Tapes that have been used longer than two years shall be discarded and replaced with new tapes.
- **Responsibility:** IT team will perform regular backups. A designated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.
- **Log File:** A log file is kept for backup purposes which will record every successful/unsuccessful backup activity. Any failure recorded in the logs, should be immediately reported to the Head IT.
- **Testing:** Restoration of data from backups shall be tested at least once per month.
- **Data Backed Up:** Systems to be backed up include but are not limited to:
    - File server
    - Production database server
    - Test database server
    - Domain controllers
    - Backup Logs
    - Attendance Logs
    - Archives
- **Archives:** Archives are made at the end of every year in December. User account data associated with the file servers are archived after one month, the user left the University.
- **Restoration:** Users that need files restored must submit a request to the IT help desk. Users will be asked to include information about the name of the file, date of creation, the last time it was changed, and the date and time it was deleted or destroyed.
- **Tape Storage Locations:** Offline tapes used for everyday backup shall be stored in the library block in a fireproof safe.

○

Critical IT Incident Management

This section provides a framework for reporting and managing any major incidents that affect the operations of the IT Systems

- Any major incidents affecting the University's information and IT systems.
- Loss, disclosure, or corruption of information or devices.
- Near misses and information technology concerns.

The goal of Incident Management is to restore the IT service to its normal operation and to manage unplanned events which result in disruption of IT services:

- Interruption to the normal operation of an important IT service.
- Report or notice of a reduction in the quality of an important IT service.
- Failure of a Configuration Item (Cfg-Item) that has not yet impacted an IT service.

The aim is to support the prompt and consistent management of any major IT incidents to minimize any harm to IT services/operations of the University and reduce the risk of future breaches of IT services. To this end all users of University IT systems need to:

- Understand their roles in reporting and managing such incidents
- Report all actual or suspected incidents immediately on the following contact addresses: it.helpdesk@ashoka.edu.in, +91 130-2300314/ +91 7082000418.

The policy supporting procedures provide a clear and consistent methodology to help to ensure that actual and suspected major incidents and near misses are:

- Reported promptly and escalated to the right people who can take timely and appropriate action.
- Recorded accurately and consistently to assist investigation and highlight any actions necessary to strengthen IT controls.
- Only critical IT incidents will be reported through this process, the normal incidents/day by day calls will go through the helpdesk ticketing system.
- Maintaining adequate logs and evidence to enable investigation of incidents and preserve the chain of custody where this information is required for legal or evidential purposes.
- The University will deploy lawful and proportionate measures to protect information systems by monitoring its IT networks and systems to detect and alert staff in case of system outages

Line of Responsibility

The below is established for critical Incident Management:

- The IT team must use the currently approved documented critical incident management process and will be reported, recorded, managed, and appropriately communicated through the approved Incident Management form.
- All members of the IT team are responsible for ensuring the Incident Management Process is followed.

- Upon resolution of an incident, the end user will be notified that the incident has been resolved and restored to normal business function.
- Once the incident has been resolved, the user will have seven (7) calendar days to reopen the incident.

Compliance & Monitoring

Incidents will be reviewed on a periodic basis by the Incident Management Process Owner/Head IT/ GM IT to audit for policy compliance. The Head/GM IT will monitor and review all information such incidents and make a regular report to senior management recommending further action and along with issues and risks. This is to ensure that the procedures, guidelines, and standards set forth in the Incident Management Process are adhered to.

Review

The Incident Management section will be reviewed:

- Annually, by the Incident Management Process Owner
- Upon an update to the Incident Management Process
- Upon request of the Policy Steering Committee

Enterprise Resource Planning

Scope & Overview

The following guidelines are applicable to all users who have access to any instance of Enterprise Resource Planning (ERP) software implemented at Ashoka University since July 2015. The software implemented is Microsoft Dynamics Navision R2 2016.

This section is intended:

- To ensure that ERP system is used for its intended purpose
- To ensure the integrity, reliability, availability, and performance of ERP system

This section covers the following aspects of the Enterprise Resource Planning (ERP) software implemented at Ashoka University:

- Logical Access and Controls
- Change Management and Controls

The University has an ERP review committee which periodically reviews and approves all the changes to user access, logical access controls and change management. The committee includes individual custodians of the following modules of enterprise resource planning software.

Committee Member	Designation
Custodian of Purchase Module	Head of Purchase
Custodian of Finance & Accounts	Director, Finance

Custodian of Human Resource (HR)	Director, Human Resource (HR)
Custodian of System Administration & Education	Director, Information Technology & Systems (IT&S)

Maintenance, Testing and Deployment

All development, maintenance and testing activities are carried out by the developers of the vendor deputed for the same (Corporate Serve). The Information Technology team oversees the implementation of the change requests approved by the review committee.

The following environments have been set up for the Navision implementation at Ashoka University.

- **Development Environment:** The consulting developers have access to the license's development environment of Microsoft Navision.
- **User Acceptance Testing Environment:** All users of ERP have access to a replica test instance of the production environment for user acceptance testing of the changes.
- **Production Environment:** All approved users of ERP have access to the production environment of ERP. The production instance has four companies:
    - Ashoka University –Live
    - IFRE-Live
    - Vasant Kunj
    - IFRE-FCRA

The change request is closed after completion of user acceptance testing and signed off by the ERP system administrator. The objects are then migrated to the production environment.

User Access Controls

New Users: Once a new employee joins the University and the HR department has created the employee in the system, the IT team creates an active directory ID for the employee.

- **Access Authentication:** Navision allows two authentication mechanisms:
    - **Local Authentication:** The user is provided with a user ID and password to access the instance of Navision.
    - **Active Directory Authentication:** The user can access the instance of Navision from his Active directory credentials.
- Ashoka University uses active directory authentication
- **Access Request:** User sends the email to ERP systems administrator requesting the change required with the approval of department head or ERP review committee.
- **Logical Access Controls:** Once the access request is completed, the ERP systems administrator completes the following user setup in Navision
- **User Access:** A new user is created, and authentication is linked to the user's active directory ID.
- **Role Center:** A role Centre is a combination of pages, permissions, and user personalization.
- Permissions control the read, write, and execute permissions on the tables and pages.

- User personalization controls the pages that can be accessed by the User Interface.
- Customized role centers (permissions & personalization) have been created by the development vendor and are assigned to the user by the systems administrator.

If the role center is not present, then the system administrator creates a change request for the new role after getting an approval for the same by the review committee via email.

Existing users

- **Modification Request:** A request must be made by the user or his/her department head for the change in user access over an email.
- **Approvals:** The change request must be duly approved by the department head or member of ERP review committee.
- **Multiple Accounts:** Existing users can have multiple accounts to access multiple stores. For such an exception, the review committee approves the request.

Inactive Users

- **Deactivation Request:** ERP systems administrator deactivates the account upon receiving the information from the user's Head of Department (HoD) or ERP review committee.
- **Exit Deactivation:** Employees marked inactive by HR are deactivated from the system by the system administrator once notified by HR by providing a copy of the exit form of the employee.

Super Users

- ADMINISTRATOR: The ID used by the network administrator responsible for maintaining the application and database.
- CORP: The ID used for the installation and update of Navision by the vendor
- ERP DEVELOPER: The ID used by the vendor
- ERP MIGRATOR: The ID used by the vendor

Change Management Controls

All Application development and changes are broadly categorized as follows:

- **Category-Process Change:**
  - All new development includes any change in either of the following
    - Logical Access
    - Permissions & Role Centre Customizations
    - Process Changes
    - Enhancements to existing process
  - The change requests are submitted to the systems administrator by the current ERP users over email.
  - Once approved, the changes are notified to the vendor over email.
  - The changes are then developed in the development environment and objects are moved to a test instance for the user acceptance testing by the requesting user.
  - Once the testing is completed, the changes are migrated to the production instance.

- **Category-User Experience (UX):**
  - All maintenance activities include a change in either of the following

        - Bug Fixes
        - Reports
        - Tasks
        - UI Design
    - The change requests are submitted to the systems administrator by the current ERP users over email.
    - The changes are notified to the vendor over email.
    - The changes are then developed in the development environment and objects are moved to a test instance for the user acceptance testing by the requesting user.
    - Once the testing is completed, the changes are migrated to the production instance.

- **Emergency Changes**
    - All changes which are critical for business continuation and where the approver is not readily available, system administrator can initiate the change request and get the changes live in the production server.
    - In such cases the post facto approval will be recorded once the approver is available.

- **Change controls review:**

All change controls are reviewed once every quarter by the present members of the review committee

Policy Review

This policy may be periodically reviewed and modified by the respective Department Head(s), who may consult with relevant committees, faculty members, students, and/or staff of the University.

The latest version of the policy will be always available on MyAshoka (See: https://my.ashoka.edu.in) and is subject to change during the periodic policy review undertaken by the University. Please visit the MyAshoka Portal to review the latest up to date IT policy.