



## **eGovernance@ LEAD**

# **Consolidated Report for 2021-23**

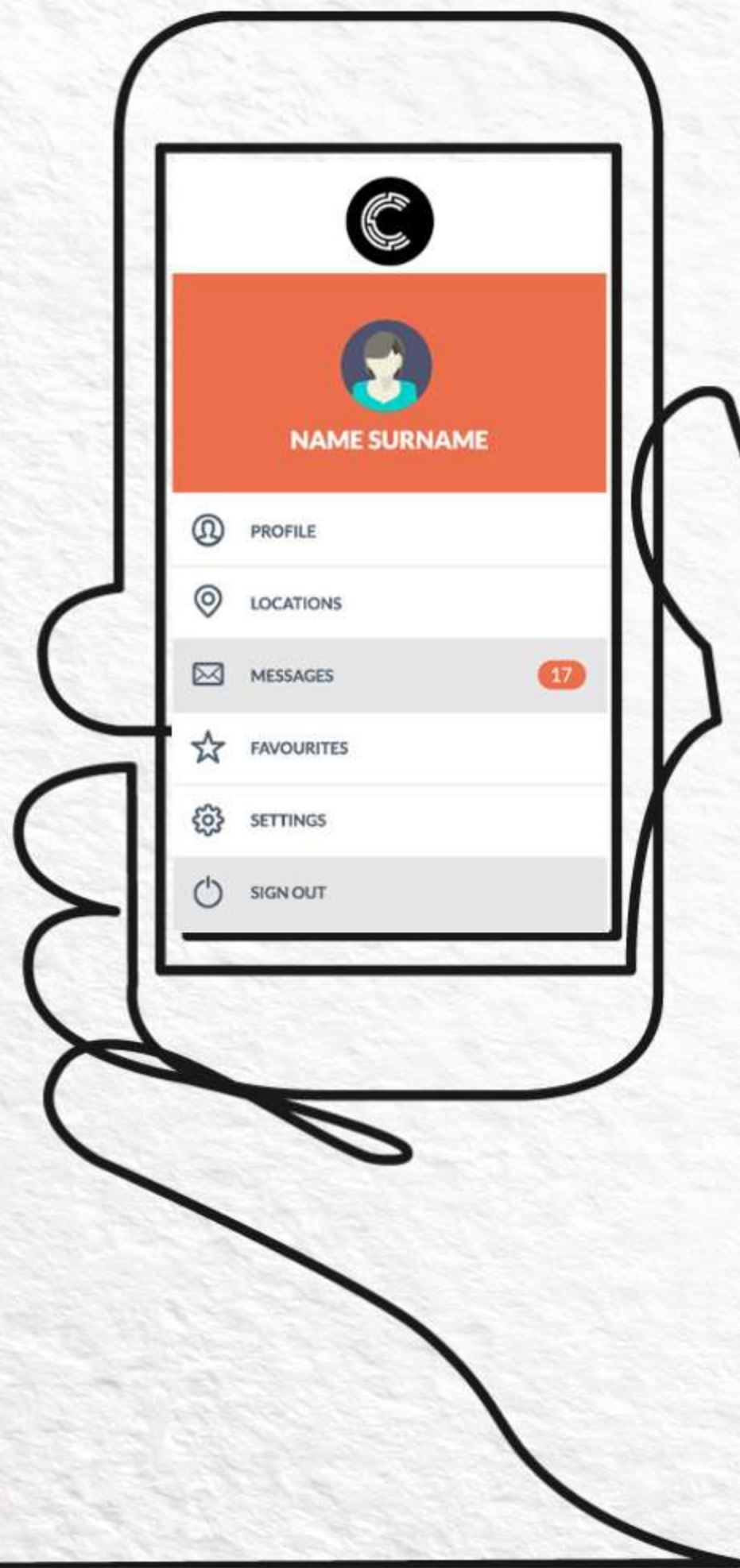
LEAD COLLEGE OF MANAGEMENT  
PALAKKAD, KERALA  
SEPTEMBER 2023

## Table of Contents

1. The eGovernance Policy@LEAD
2. DMG DIRECTIVES FOR THE POLICY DEPLOYMENT
3. REPORT FOR THE YEAR 2022-2023
4. REPORT FOR THE YEAR 2022-21
5. REPORT FOR THE YEAR 2020-21
6. IS POLICY ( ISO 21001:2018)

  
Ms. Yasmin Samad  
Administrative Head





# eGovernance@LEAD

**POLICY, GUIDELINES AND MANDATES**

# LEAD

LEAD COLLEGE OF MANAGEMENT

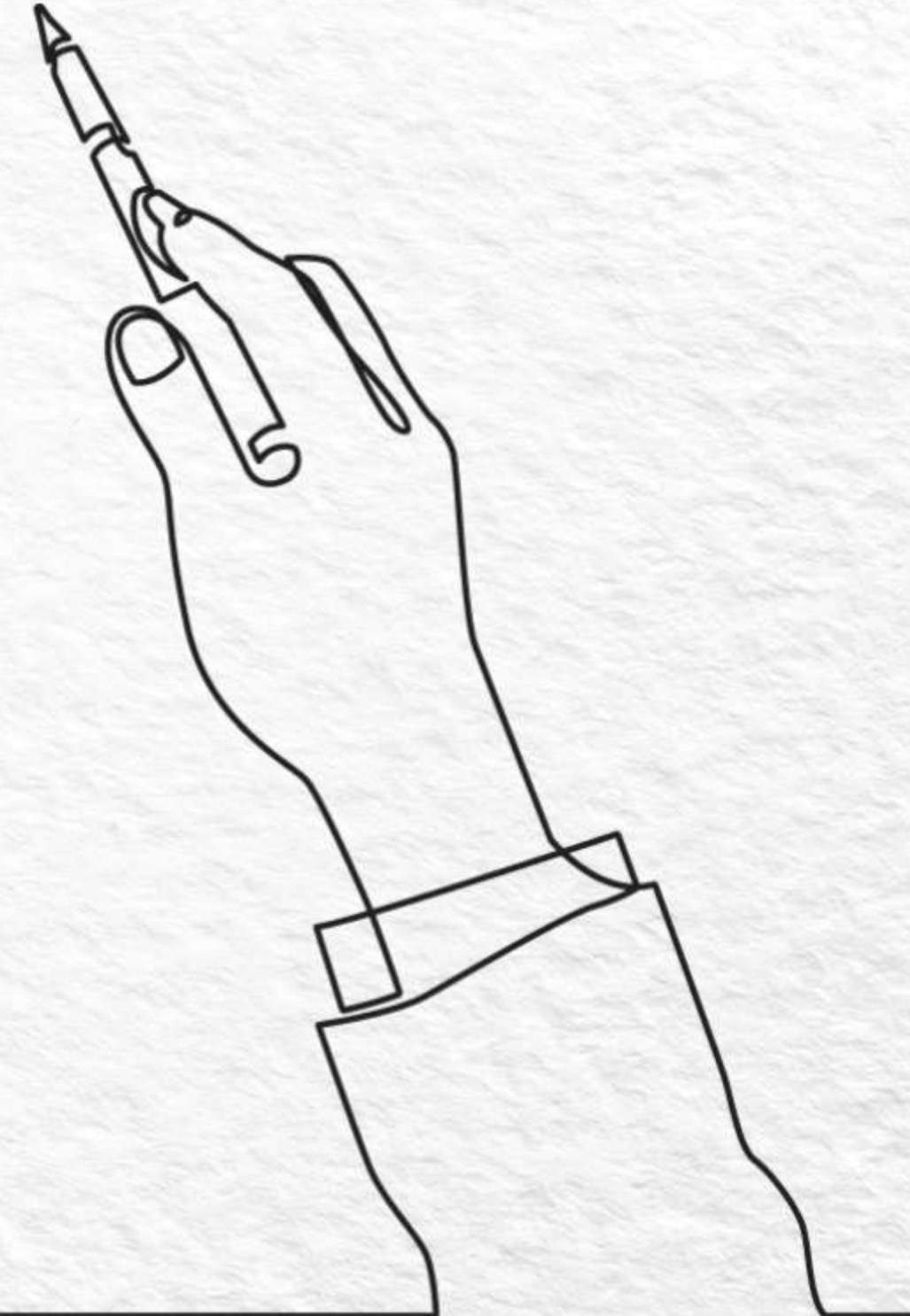
**VERSION 2021-22: NEXT REVIEW : 6/24    ISO21001:2018 REVIEW**





# Contents

- ➔ Introduction
- ➔ The Core Principles
- ➔ Overview
- ➔ eGovernance At LEAD
- ➔ Plan Outline for 2022-23





# Introduction

As we recover from the pandemic and achieve some semblance of normalcy, we have also learnt a few lessons to deal with this new normal.

- a. Our dependency on ICT and related technology is going to be substantive.
- b. Developments in education technology has meant that there are more opportunities to create excellence in teaching-learning, course development and indeed managing the entire education journey of our students leveraging software and technology.
- c. Enhancing education processes, its management and control, review and managing information all now focus on using technology and platforms.

This document is a policy statement for LEAD College of Management as to what eGovernance entails at LEAD and what are the directives, challenges, deployment and plans to ensure a robust system is in place. This is to be read in conjunction with "Establishing digital enablement and enhancement at LEAD College of Management.POLICY GUIDELINES" issued by Decision Making Group (DMG) in January 2021 as a precursor.

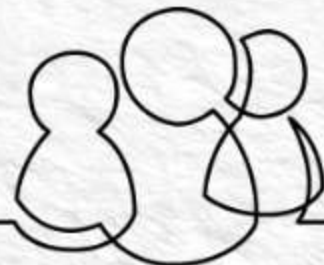
We have just applied for NBA accreditation and have started work on NAAC 2nd cycle. Alongside, the IQAC team is preparing the groundwork to start the ISO 21001:2018 certification. Over the next 3 years we expect to complete all these.

The Decision Making Group has mandated that the operating principles should be based on the acronym: STRATA: The tools, software and the processes we use must ensure **Security**, be **Trustworthy** and **Reliable, Accountable** and remain **Transparent** and **Accessible** to our stakeholders.

I am also pleased to say the the DMG has always supported us in our endeavours to support technology deployment by our student stakeholder through a special "Laptop" and "Smartphone" scheme for deserving students where grants are given to them to purchase them. Over the past 3 years we have awarded over Rs. 30 lakhs under this scheme and a similar amount is planned for 2022-24



Dr. Thomas George K  
Director  
November 18, 2021





# THE CORE PRINCIPLES



## SECURITY

Hardware and software access , data storage, antivirus and firewalls. Encryption.



## TRUSTWORTHY

Deployed manpower, service provider and data/records validated



## RELIABILITY

Low failure rate, replicability and continuity of uninterrupted service, accuracy



## ACCOUNTABILITY

Ownership of data, auditm validation and assurance of error-proof and uncorrupted data



## TRANSPARENCY

Open to access and availability on need-to-know- basis, comprehensible dashboards and clear SOPs and error mitigation processes in place.



## ACCESSIBILITY

Easy access to data, saving paper, preserving information , creating knowledge repository





LEAD is a full residential business school and is expected to have an annual student strength of 720+ by 2024. Apart from this there will be 100+ faculty and non teaching employees on board.

To ensure that there is a continuous improvement, enhanced efficiencies in our processes and quality management, there is a need to:

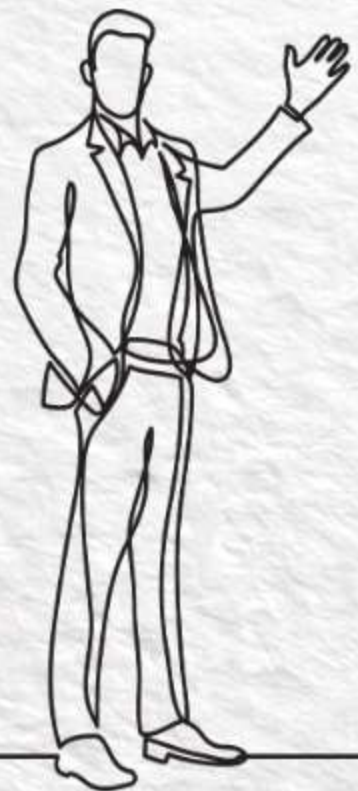
- a. Automate processes where possible to expedite tasks
- b. Leverage technology to deliver teaching - learning excellence.
- c. Deploy applications and capture value from social media and internet space
- d. Establish secure systems to ensure that the ISO:21001:2018 guidelines are followed in letter in spirit

This will not only save paper but help in preserving information, create better monitoring and improvement opportunities and will ensure that we remain proactive.

The Decision Making Group has reviewed the NBA SAR and has conducted an audit of current practices of eGovernance.

The group has identified the areas to focus on as a value chain for LEAD College of Management. Some indicative areas are:

- i. Pre-Admission/Admission Processes: Both CRM, application process and communications should be paperless and deliver reports status in real-time.
- ii. Academic processes: attendance, course plans, time-table, scores, leave processes for students to be managed through a suitable LMS/portal-based system. Placement process and management to be application driven,
- iii. Administration: Faculty and staff attendance, documentation, leave processes to be automated with a dashboard and suitable attendance recording system. All financial transactions including receipts and payments should be digital and suitable QR codes etc. to be displayed and used with a system to create e-receipts.
- iv. Services: Library automation in terms of attendance, library management software, IT-services to be enabled with firewall and sensitive PCs/Laptops to have additional security layers, security cameras in the campus with proper recording and management to be in place
- v. Branding: website, social media sites to be managed and updated to ensure information currency





# eGovernance@LEAD

## PLACEMENT

CRM software to be deployed, Extending ZOHOCRm licence. GD/Pi video recording system to be in place as smart class extension. Online testing by third party ( e.g. SHL-AMCAT to be evaluated.

## BRANDING

Separate team to manage digital marketing, website and social media platforms , e-newsletters and setting up of youtube channels and equipment upgrade for video/photography

## SERVICES

Enhancing library e-resources with selected e-books for electives. Creating repository of video-lessons and revision notes. Enhancing IT infrastructure by way of hardware, bandwidth, devices and cameras to be completed to increase footprint to 700 students planned end 2023. Additional qualified manpower hire



## ADMISSIONS

- \*Seamless application process through website
- \*CRM software to capture marketing and process
- \*Evaluation and selection process enabled software
- \*Current process uses ZOHOCRm platform
- \*WhatsApp management through PC/Laptop as secondary data support

## ACADEMICS

- \*Class Management : Time table, attendance capturing, outcomebased education mapping, student feedback and internal marks management through "Linways" LMS
- \*Plagiarism detection application to be installed

## ADMINISTRATION

Enhanced security for devices logging on to online banking. Facial recognition software and device for employee in place. IS policy and digital engagement policy in place. Audit for 2021 completed.



# Plan Outline 2022-23



## ADMISSION

ZOHOCRm is to be deployed. Automated software including mailchimp to be evaluated. WhatsApp as an institutional account to be created. Online application forms, payments and receipts to be further improved. Admission call center reports to be a part of ZOHOCRm suite. All marketing collatorals where possible should be in soft copy form and hard copy to be kept at a minimum if not avoidable.

## ACADEMIC

Linways has been deployed, A full LMS and academic management system to be put in place with applocation upgrade or to consider other providers like Canvas. Moodle deployment to be examined as it can be comprehensive. Attendance systems using higher technology like FRS to be deployed at class room level. New AI technology to be explored to leverage facial recognition. ERP based solution to be examined. University Portal and data to be managed and secured

## SERVICES

Facial Recognition Attendance system to be tested and deployed for all faculty and staff attendance. ESS to be evaluated. Library software to be upgraded to open source \_ KOHA to be implemented. Bar code scanners to be installed for attendance recording. Additional digital resources like databases, joournals to be added ICT enabled classrooms with smartboards and integrated AV system and software to be deployed. Vendor demonstrations to be initiated in 2022.

## BRANDING

Website audit and updation on 3-month cycles. Additional documentat=ion and landing pages for quality. Updated reports for admission and placement to be included in the website. Moving to wordpress planned for 2022-23. Separate team to operate the social media platofrms and websites.

## COMPLIANCE

ISO21001:2018 Information security Policy to be in place. Draft to be approved and integrated with the next annual eGovernance plan. Plagiarism software as indicated in the digital enhancement statement of January 2021 to be deployed.





## Decision Making Group LEAD College of Management

### Re : Establishing digital enablement and enhancement at LEAD College of Management.POLICY GUIDELINES

The subcommittee of the board of governors has reviewed the draft document on the IS Policy released by IQAC in connection with the ISO 21001:2018 standards.

The objectives are to ensure transparency, trust and accountability in governance at various levels and ensure that all records and processes are recorded with accuracy and monitored whilst ensuring security of data and information stored.

The following recommendations have been made for immediate implementation where possible and not more than within a 6 month/semester period.

1. **Administration :Faculty/Staff attendance , leave management processes:** These are currently done manually. The recommendations are to install an ESS attendance system

- i. Installing a facial recognition/fingerprint system for login and logout.
  - ii. As additional backup an attendance register and a day-movement register to be in place.
  - iii. By 2024 , ID cards must be chip enabled, carry ID Nos and contain QR codes for digital signatures of both the employees and the HR/Director signature.
  - iv. At least 3 office staff to be trained in managing this system.
  - v. SOP for leave applications etc. need to be strengthened.
- IT consultants have recommended installing an ESS system and are reviewing suitable providers for selection.
  - It is recommended a one time-budget in the range Rs.10 lakhs be provided with an annual recurring cost .

2. **Admission Management Processes:** DMG has recommended that we move from traditional google documentation and adopt a reliable CRM software for managing the program marketing, admission administration and management of the selection process as a dashboard is need to monitor the progress especially since the approved admission count is now 300 annually and we are planning to extend this to 360 by 2024. The marketing team should be trained to use it.

- We have been offered Zoho CRM from our alumni entrepreneur and are currently testing it.
- Deployment is ongoing
- The estimated one time cost is expected to be between Rs.5-7 Lakhs with an annual recurring cost of Rs. 1.0 lakh .

3. **Student Management system:** Whilst we are having a basic version of the Linways, it does not provide for additional deployment to create a 360 degree LMS and help prepare for a technology-enabled transparent system. The institute should ensure there is re-training for faculty and staff as the need is to have a robust attendance management for students, reports from which can be viewed by students and other key stakeholders, assessment management systems with marks, scores are entered and mapped to outcome based education is possible

- The recommendation is to upgrade the current system being used and consider adding modules where possible



- In the larger framework by 2024 we plan to go for smart class rooms, there may be a need to migrate to a higher level/ERP and MOODLE transition needs to be examined.
- The current one time cost incurred is Rs 3-4 Lakhs with an annual recurring cost of Rs 1 lakh is being incurred
- The suggested transition for 2024 is expected to have one time cost and is expected to be between Rs.10-12 Lakhs with an annual recurring cost of Rs 3.0 lakhs

3. Supplementing the above, there is also the university portal for LEAD which needs to be constantly updated, corrected and attended to where access is enlarged and all key stakeholders are going to access the portal for data including students. For better understanding and governance DMG has suggested faculty training /workshop in late 2023 early 2024 when we update faculty and student data into the portal. The portal access and use fees are included in the annual payment we make for affiliation annually.

4. Real time session wise attendance recording for students.: As the institution grows in size and we expect a student strength of 720+ in the campus and a 12-14 batch classroom configuration, session wise attendance taking before and end of each class will be time consuming and eventually faculty have to enter data into Linways. The institute should consider deploying FACIAL RECOGNITION SYSTEMS for this and for students, preferably with geo-location in place. Attention should be paid to IS policy and information security protocols.

- We have initiated a collaborative project for deployment and execution of this with a startup whose team is working with us. An investment of Rs 10.0 is earmarked and testing is ongoing and it is expected that the integration of this will be possible by November 2023

5. There is also a mandate to ensure that plagiarism detection software is in place, at least for work which is summative and needs quality and ensure possibility of publications of projects and for faculty to ensure their papers pass the test. Turnitin is the key provider and the suggestion is that LEAD acquires a few licenses to start deploying and gaining experience and then engage in full deployment. This will be essential from an autonomy point of view.

- We will check with the university. IQAC has recommended Ouriginal (earlier Urkund which was bought out by Turnitin)
- The estimated annual license cost is expected to be between Rs 3.5 lakhs and Rs 5.0 lakhs based on functionality with Ouriginal costing approximately 30% less

6. Financial transactions and record -keeping is currently managed through Tally 9.0 which may be upgraded to Tally ERP.

7. The Internet system is firewalled (SOPHOS). However additional software for security should be considered for security, especially for devices which share, store and process sensitive and "at-risk" data e.g bank applications, university and other portals. Therefore add-on anti-virus software is recommended for computers identified as high risk in administration, exams, accounting functions.

8. There is a need to add more surveillance cameras around and inside the campus as we increase our infrastructure. This network should be comprehensive whilst ensuring no breach of personal privacy rights. The new hostel blocks and additional security points need to be covered. The data capture and storage policy should be mandated with adequate backup and security to be provided. The system should also have an application based access for remote viewing and off -site monitoring especially for nights.



- Currently we have 40+ cameras in place and in 2023-24 cycle additional 20+cameras to be reinstalled/ installed .
- An additional one time expense of Rs.5 Lakhs and an annual cost of Rs. 1 Lakh is envisaged.
- Once FRC is in place we will examine upgrading cameras at entry and exit points to capture in-campus and out-of-campus movements.

9. Technology enabled classrooms and ICT enablement including use of “ smart technology” is now almost mandated . The recommendation from the BoG is the following:

- Upgrade of current 10 classrooms to be completed by November 2023 in addition to smart screens at Boardroom and Kalam Hall.
- Creation of a pack-and-go digital recording kit to capture microsession, create/capture teaching and other learning and teaching digital materials. In addition hardware and software to create learning channels / repositories.

In summary the approval for the categories are listed below

( In Rs. Lakh total for the year including recurring expenses)		
Item	2023-24 requirement	2024-25 requirement
Administration:HR management, FRC	3	2
Admission management process	3	2
Student mgmt system including Moodle/Linways upgrade	5	5
Realtime attendance system, AI FCR	10	3
Plagiarism detection	4	4
Anti virus software	1	1
Surveillance system upgrade	5	5
Smart classroom upgrade	15	10
Additional requirements not covered above.	5	5
TOTAL	51	37

We will report to the BoG the progress in the Jan 2023 cycle and send an update by November 2023



Director  
Jan 21, 2022





## AUDIT AND PROGRESS REPORT ON E-GOVERNANCE AT LEAD COLLEGE OF MANAGEMENT: 2022-23

To: The Trustees  
 Prompt Charitable Trust  
 Palakkad

This is a summary of the activities and progress on implementation of the e-governance at LEAD College of Management for the period 2021-22. The report was prepared by the IQAC team and coordinated by Dr. Umesh Chandrasekhar, Professor who has substantive industry and academic experience especially in national and international accreditations and outcome based education. We also now have an IT support team headed by Ajai CK, an industry veteran.

Post review of 2021-22 several changes have been made and more are expected. The IS policy for ISO 21001:2018 is now in place and LEAD is certified. The admission for the year, as anticipated, has been 300 and currently there are 600 full time residential students in the campus.

The management has undertaken since 2021 major infrastructure development including construction of a new boys hostel , a third canteen-kitchen service block and extensive landscaping is being undertaken

No	Item	Investment if any	Comments
1	Board of Governors	Rs 4.00 lakhs	The Board has been reconstituted and has a cross section of academic and industry leaders. Two meetings have been held and these have been digitally captured and minutes and reflect points of reference for e-governance also.
2	LMS enhancement	Linways, Cost TBA	More reporting systems added including leave application digitisation and approval systems.
3	Classroom attendance	Estt Rs 10-25 lakhs	LEAD is creating a proprietary application which is AI driven remote facial recognition and to be installed in all classrooms and at exit points to track attendance and in-campus presence. Additional bandwidth and hardware upgrade is ongoing. Testing at 2 classrooms indicates reliability. Security of data and record holding to be directed by IS policy
4	E-Learning	Rs. 20-20 lakhs	All classrooms to be “smart” and installation is complete and to be fully operational with hybrid and recording of sessions by November 30th. Faculty training ongoing
5	Anti-virus software	NA	six PCs in administrative areas were identified as vulnerable and additional anti-virus/phishing software for them and 4 LEAD owned smartphones installed

Additional observations:



- Linways version updated. Given the scale, we are recommending a fuller version or a shift to another vendor like Canvas etc as these are more user-friendly.
- JASP statistical software now installed in the Lab. Capacity for PCs now 100.
- Mandatory ERP/SAP training to be conducted in January 2023
- To enhance digital engagement and to encourage online learning, moocs, LEAD College of Management has reimbursed laptops and smartphones worth Rs. 33 lakhs this period which has benefitted over 100 students to empower them and remove dependency on IT lab and provide online learning mechanisms even at hostels.
- Additional investments have been made for bandwidth, server capacity, computer lab and software.
- Negotiations are on with Urkund and other plagiarism software (turnitin) to deploy this in the LMS now concluded. License from Turnitin now in place on trial basis.
- Post completion of infrastructure work, major overhaul of IT infrastructure and reconfiguration is planned early 2024.
- There is also a proposal to initiate a mini-studio "Taranga" which will create content, micro-lessons and train faculty for virtual /hybrid teaching and manage content and web assets.

"Tests" on the IT infrastructure to ensure that the systems are secure were conducted.

Effective September 2023, Dr. Umesh Chandrasekhar will take over this role as he now heads quality assurance and accreditations and is the designated MR for ISO.



Ms. Yasmin Samad  
Administrative Head  
August 2023



cc.DMG , Dr. Balamourugane, Dr. Thomas, Dr. Umesh  
Chandrasekhar File in DMG folder






AUDIT AND PROGRESS REPORT ON E-GOVERNANCE AT LEAD COLLEGE OF MANAGEMENT:  
2021-22

To: The Trustees  
Prompt Charitable Trust  
Palakkad

This is a summary of the activities and progress on implementation of the e-governance at LEAD College of Management for the period 2021-22. The report was prepared by the IQAC team and coordinated by Dr. Balamourgane. Post review of 2020-21 several changes have been made and more are expected. The DMG directive and the e-governance policy has been released along with the draft IS policy for ISO. The admission for the year, as anticipated, has increased to 300 and currently there are 480 full time residential students in the campus.

No	Item	Investment if any	Comments
1	Additional software purchase including ZOOM licences , renewals and antivirus software for the period 2019-21	Rs 11.80 lakhs	includes software upgrades. New faculty need orientation and training in Linways
2	Hardware upgrades and IT security and maintenance	Rs. 3.36 lakhs	Hostels wifi enhanced. Additional CCTV cameras were installed.
3	Digital Payment		Federal Bank QR codes in place now and being used for all payments including fines etc. BHIM in place via SBI
4	Attendance system	TBA	The ESS attendance





			software has now been installed and is being tested. Classroom attendance through similar “fingerprint/facial” recognition is not fast enough and attendance has to be taken for approximately 500 students session wise in-out basis 8 times a day. A new mode is called for.
5	Library system	Ebase being used	Koha deployment . This will take time and will be rolled out in late 2022/ early 2023. New Librarian Dr. Pratheepa has now joined and is leading the initiative including an automated attendance system for library users.
6	Website and social media platforms	Rs 5.0 lakhs	The audit has shown several weaknesses in terms of organizing the information, information currency and user-friendliness. A team of 3 is being set up in December 2022 to review and revamp the sites and portals. Alumni has own website almashines which need updates.

Additional observations:

- Admissions ZOHO CRM fully operational now. All documentation now digital including data capture
- Mandatory ERP/SAP training now in place for all students as a value-added program
- To enhance digital engagement and to encourage online learning, moocs, LEAD College of Management has reimbursed laptops and smartphones worth Rs. 26 lakhs this period which has benefitted over 100





LEAD COLLEGE OF MANAGEMENT  
Accredited by NAAC

Approved by AICTE and Affiliated to University of  
Calicut


Dhoni, Palakkad, Kerala, India – 678009,  
Ph: 0491 2553693, Mob: +91 9497713693  
Website: [lead.ac.in](http://lead.ac.in) Email ID: [info@lead.ac.in](mailto:info@lead.ac.in)



students to empower them and remove dependency on IT lab and provide online learning mechanisms even at hostels.

- Additional investments will be required to expand bandwidth, server capacity, computer lab and software.
- Smart classrooms are now mandated and we need to upgrade to this at the earliest - More progress to be initiated post NBA comments
- A separate Decision Making Group meeting advisory and policy in place now
- proposed ISO 21001:2018 certification documentation and IS policy draft is ready and being circulated
- Negotiations are on with Urkund and other plagiarism software (turnitin) to deploy this in the LMS
- Two more staff including an IT expert to be hired as per DMG directive. They are expected to join in early 2023.

There is a need to conduct “tests” on the IT infrastructure to ensure that the systems are secure.

  
Ms. Yasmin Samad  
Administrative Head  
September 2022

cc.DMG , Dr. Balamourugane, Dr. Thomas File in DMG folder







AUDIT AND PROGRESS REPORT ON E-GOVERNANCE AT LEAD COLLEGE OF MANAGEMENT:  
2020-21

To: The Trustees  
Prompt Charitable Trust  
Palakkad

This is a summary of the activities and progress on implementation of the e-governance at LEAD College of Management for the period 2020-21. The report was prepared by the IQAC team and coordinated by Dr. Balamourgane. On account of virtual learning deployment for 2020-21 and some parts of 2019-20 several steps were taken

No	Item	Investment if any	Comments
1	Additional software purchase including ZOOM licences , renewals and antivirus software for the period 2019-21	Rs 11.80 lakhs	includes software upgrades
2	Hardware upgrades and IT security and maintenance	Rs. 3.36 lakhs	PCs from which external data, banking etc. is accessed and needed secure configuration
3	Digital Payment	None	All transactions barring petty cash items are now digital. A few student fees are being received as DDs on account of bank loan processes. We are trying to centralise this to get digital/ UPI qr codes in place.
4	Attendance system	TBA	The current system needs to be replaced and this is planned for 2022-23. Negotiations and vendor evaluation is ongoing
5	Library system	Ebase being used	The audit recommendation is to go for Open Source software e.g. Koha . This will take time and will be rolled out in late 2022/ early 2023





LEAD COLLEGE OF MANAGEMENT  
Accredited by NAAC

Approved by AICTE and Affiliated to University of  
Calicut

Dhoni, Palakkad, Kerala, India – 678009,  
Ph: 0491 2553693, Mob: +91 9497713693  
Website: [lead.ac.in](http://lead.ac.in) Email ID: [info@lead.ac.in](mailto:info@lead.ac.in)

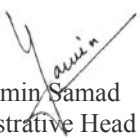


Additional observations:

- Several new faculty members need to be trained and additional re-training has to be given on the Linways LMS. This is to ensure that we create a robust outcome based education reporting system and manage attendance and leave application processes seamlessly. This will mean additional investment in software upgrades.
- There are some concerns about the security cameras location and safety of recordings. The cameras in the girls hostel will be repositioned . Additional cameras will be installed at some “black spots’ identified by the team.
- Placement activities also need to espouse a CRM application and progress tracking and management. They have been asked to test ZOHOCRm also which we have recommended for managing admission processes.
- To enhance digital engagement and to encourage online learning, moocs, LEAD College of Management has reimbursed laptops worth Rs. 10.5 lakhs over a two year period which has benefitted over 60 students.

We are also planning to increase the current intake from 180 to 300 students from academic year 2021-22.

Additional investments will be required to expand bandwidth, server capacity, computer lab and software. Smart classrooms are now mandated and we need to upgrade to this at the earliest. A separate Decision Making Group meeting has been called for in January 2022 to finalise the e-governance policy and investment directions prior to the NBA visit. This will also have to be in line with the proposed ISO 21001:2018 certification for which ground work will begin next year and we hope to progress and achieve this in early 2023.

  
Ms. Yasmin Samad  
Administrative Head  
July 9, 2021

cc.DMG , Dr. Balamourugane, Dr. Shankar Ganesh. File in DMG folder





## **Information Security Management System Policy**

The following information security principles provide overarching governance for the security and management of information at LEAD College of Management.

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability and in accordance with relevant legislative, regulatory and contractual requirements.
2. Staff with particular responsibilities for information must ensure the classification of that information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.
3. All users covered by the scope of this policy must handle information appropriately and in accordance with its classification level.
4. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.
5. Information will be protected against unauthorised access and processing in accordance with its classification level.
6. Breaches of this policy must be reported
7. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits and penetration testing.
8. Any explicit Information Security Management Systems (ISMSs) run within the LCM will be appraised and adjusted through the principles of continuous improvement.



Dr. Thomas George K  
Director





## Information Security Policy

### ISO:21001:2018 Guidelines and Processes Version : I of October 2022.

Table of Contents

3



This is a property of LEAD COLLEGE OF MANAGEMENT and cannot be reproduced without prior permission

A blue ink signature of Dr. U. Chandrasekhar.

A green ink signature of Dr. Thomas.



## Information Security

Updated: 26.10.2022 Issued By: IQAC Team Owner: Administration Heads

### Introduction:

**Lead College of Management ( LCM) is a stand-alone, fully residential affiliated business school with an annual intake capacity of 300. A two-year full-time MBA is offered.**

**Information is maintained in hard and soft formats and calls for effective management to ensure secrecy where needed, security against data breach and tampering and effective backups and system redundancies to ensure there is recourse to data in the event of any adverse event. There is an IT usage policy in place at LCM. This document addresses Information Security at LCM.**

### 1.0 Purpose and Benefits

This policy defines the mandatory minimum information security requirements for LEAD College of Management as defined below in Section 3.0 Scope. Any entity may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy.

This policy acts as an umbrella document to all other security policies and associated standards. This policy defines the responsibility to:

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- assure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions and vital government functions; compromise data; and result in legal and regulatory non-compliance.

This policy benefits LCM by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.

### 2.0 Authority

LEAD College of Management is a full residential campus with 700 stakeholders and the model is an oil-rig model with 40 days nonstop work with a 10 day break. Information processes is the core activity we do, it is strategic and determines multiple outcomes for almost all our stakeholders including faculty, students, recruiters, management, university and society at large. It is cyclic, needs constant improvements to ensure we remain competitive, relevant and innovative to ensure both in terms of learning outcomes and academic vigor. This process has been identified as a critical area marked for improvement by the management . Data held by LCM is varied over a longer time-frame and is evidentiary in nature for ISO/NAAC and other critical accreditation parameters. Data/information presented as outcomes/grades/scores are critical from






management, institution, university and student stakeholders and hence need careful monitoring and management.

### 3.0 Scope

This policy encompasses all systems, automated and manual, for which LEAD College of Management has administrative responsibility, including systems managed or hosted by third parties on behalf of the entity. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

### 4.0 Information Statement

#### 4.1 Organizational Security

a. Information security requires both an information risk management function and an information technology security function. Depending on the structure of the entity, an individual or group can serve in both roles or a separate individual or group can be designated for each role. It is recommended that these functions be performed by a high-level executive or a group that includes high level executives.

1. Each entity must designate an individual or group to be responsible for the risk management function assuring that:

- i. Risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise with regard to the overall strategic goals and objectives of carrying out its core missions and business functions; and
- ii. The management of information assets and information system-related security risks is consistent, reflects the risk tolerance, and is considered along with other types of risks, to ensure mission/business success.

2. Each entity must designate an individual or group to be responsible for the technical information security function. For purposes of clarity and readability, this policy will refer to the individual, or group, designated as the Information Security Officer (ISO) designated security representative. This function will be responsible for evaluating and advising on information security risks.

b. Information security risk decisions must be made through consultation with both function areas described in a. above.

c. Although the technical information security function may be outsourced to third parties, each entity retains overall responsibility for the security of the information that it owns.

#### 4.2 Functional Responsibilities

4.2.1 Executive management is responsible for:

1. evaluating and accepting risk on behalf of the entity;
2. identifying information security responsibilities and goals and integrating them into relevant processes;
3. supporting the consistent implementation of information security policies and standards;
4. supporting security through clear direction and demonstrated commitment of appropriate resources;
5. promoting awareness of information security best practices through the regular dissemination of materials provided by the ISO/designated security representative;
6. implementing the process for determining information classification and categorization, based on industry recommended practices, organization directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;
7. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;




8. determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;
9. participating in the response to security incidents;
10. complying with notification requirements in the event of a breach of private information;
11. adhering to specific legal and regulatory requirements related to information security;
12. communicating legal and regulatory requirements to the ISO/designated security representative; and
13. communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

4.2.2 The ISO/designated security representative is responsible for:

1. maintaining familiarity with business functions and requirements;
2. maintaining an adequate level of current knowledge and proficiency in information security through annual training sessions and at new faculty induction, related to information security;
3. assessing compliance with information security policies and legal and regulatory information security requirements;
4. evaluating and understanding information security risks and how to appropriately manage those risks;
5. representing and assuring security architecture considerations are addressed;
6. advising on security issues related to procurement of products and services;
7. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;
8. disseminating threat information to appropriate parties;
9. participating in the response to potential security incidents;
10. participating in the development of enterprise policies , standards that considers the entity's needs; and
11. promoting information security awareness.

4.2.3 IT management is responsible for:

1. supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;
2. providing resources needed to maintain a level of information security control consistent with this policy;
3. identifying and implementing all processes, policies and controls relative to security requirements defined by the business and this policy;
4. implementing the proper controls for information owned based on the classification designations;
5. providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);
6. fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and
7. implementing business continuity and disaster recovery plans.

4.2.4 The workforce is responsible for:

1. understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted;
2. protecting information and resources from unauthorized use or disclosure;
3. protecting personal, private, sensitive information from unauthorized use or disclosure;
4. abiding by Acceptable Use of Information Technology Resources Policy
5. reporting suspected information security incidents or weaknesses to the appropriate manager and ISO/designated security representative.






#### 4.2.5 The CISO is responsible for:

1. providing in-house expertise as security consultants as needed;
2. developing the security program and strategy, including measures of effectiveness;
3. establishing and maintaining enterprise information security policy and standards;
4. assessing compliance with security policies and standards;
5. advising on secure system engineering;
6. providing incident response coordination and expertise;
7. monitoring networks for anomalies;
8. monitoring external sources for indications of data breaches, defacements, etc.
9. maintaining ongoing contact with security groups/associations and relevant authorities;
10. providing timely notification of current threats and vulnerabilities; and
11. providing awareness materials and training resources.

#### 4.3 Separation of Duties

- a. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.
- b. Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision.
- c. The audit and approval of security controls must always remain independent and segregated from the implementation of security controls.

#### 4.4 Information Risk Management

- a. Any system or process that supports business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.
- b. Information security risk assessments are required for new projects/software and application implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.
- c. Entities are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.
- d. Risk assessment results, and the decisions made based on these results, must be documented.

#### 4.5 Information Classification and Handling

- a. All information, which is created, acquired or used in support of business activities, must only be used for its intended business purpose.
- b. All information assets must have an information owner established within the lines of business.
- c. Information must be properly managed from its creation, through authorized use, to proper disposal.
- d. All information must be classified on an ongoing basis based on its confidentiality, integrity and availability characteristics.
- e. An information asset must be classified based on the highest level necessitated by its individual data elements.
- f. If LEAD College of Management is unable to determine the confidentiality classification of information or the information is personal identifying information (PII) the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.



- g. Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.
- h. All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.
- i. Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.
- j. LEAD College of Management must communicate the requirements for secure handling of information to its workforce.
- k. A written or electronic inventory of all information assets must be maintained.
- l. Content made available to the general public must be reviewed according to a process that will be defined and approved by the entity. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.
- m. PPI must not be made available without appropriate safeguards approved by the entity.
- n. For non-public information to be released outside LEAD College of Management or shared between other entities, a process must be established that, at a minimum:
  1. evaluates and documents the sensitivity of the information to be released or shared;
  2. identifies the responsibilities of each party for protecting the information;
  3. defines the minimum controls required to transmit and use the information;
  4. records the measures that each party has in place to protect the information;
  5. defines a method for compliance measurement;
  6. provides a signoff procedure for each party to accept responsibilities; and
  7. establishes a schedule and procedure for reviewing the controls.

Associated Standards: Information Classification Standard; Sanitization/Secure Disposal Standard

#### 4.6 IT Asset Management

- a. All IT hardware and software assets must be assigned to a designated business unit or individual.
- b. Entities are required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.
- c. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

Associated Standard: Secure Configuration Standard

#### 4.7 Personnel Security

- a. The workforce must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to specific entity sensitive information not covered in the general security training. All security training must be reinforced at least annually and must be tracked by the entity.
- b. An entity must require its workforce to abide by the Acceptable Use of Information Technology Resources Policy, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.
- c. All job positions must be evaluated by the to determine whether they require access to sensitive information and/or sensitive information technology assets.
- d. For those job positions requiring access to sensitive information and sensitive information technology assets, entities must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation or contract. Depending on the risk level, suitability determinations may include, as appropriate and






permissible, evaluation of criminal history record information or other reports from federal, state and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for LEAD College of Management to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the entity.

- e. A process must be established within LEAD College of Management To repeat or review suitability determinations periodically and upon change of job duties or position.
- f. Entities are responsible for ensuring all issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

Associated Standard: Account Management/Access Control Standard

#### 4.8 Cyber Incident Management

- a. Entities must have an incident response plan, consistent standards, to effectively respond to security incidents.
- b. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO/designated security representative as quickly as possible. If a member of the workforce feels that cyber security concerns are not being appropriately addressed, they may confidentially contact the Security Operations Center directly.
- c. The Security Operations Center must be notified of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

Associated Standard: Cyber Incident Response Standard

#### 4.9 Physical and Environmental Security

- a. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.
- b. A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary. These measures must be implemented to mitigate the risks.
- c. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.
- d. All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein.
- e. Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times.

Associated Standard: Information Security Risk Management Standard

#### 4.10 Account Management and Access Control

- a. All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and information technology (IT).
- b. Except as described in the, Account Management/Access Control Standard, access to systems must be provided through the use of individually assigned unique identifiers, known as user-IDs.
- c. Associated with each user-ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access.
- d. Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on




the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock.

- e. Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in the Account Management/Access Control Standard.
- f. Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.
- g. Tokens must not be stored on paper, or in an electronic file, hand-held device or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the ISO/designated security representative.
- h. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.).
- i. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with entity missions and business functions (i.e., least privilege).
- j. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).
- k. Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use consistent with policy, and that user activities may be monitored and the user should have no expectation of privacy.
- l. Advance approval for any remote access connection must be provided by the entity. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved and the contractual, process and technical controls required for such connection to take place.
- m. All remote connections must be made through managed points-of-entry reviewed by the ISO/designated security representative.
- n. Working from a remote location must be authorized by management and practices which assure the appropriate protection of data in remote environments must be shared with the individual prior to the individual being granted remote access.

Associated Standards: Account Management/Access Control Standard; Authentication Tokens Standard; Remote Access Standard; Security Logging Standard

#### 4.11 Systems Security

- a. Systems include but are not limited to servers, platforms, networks, communications, databases and software applications.
  - 1. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of the entity. A list of assigned individuals or groups must be centrally maintained.
  - 2. Security must be considered at system inception and documented as part of the decision to create or modify a system.
  - 3. All systems must be developed, maintained and decommissioned in accordance with a secure system development lifecycle (SSDLC).
  - 4. Each system must have a set of controls commensurate with the classification of any data that is stored on or passes through the system.
  - 5. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.
  - 6. Environments and test plans must be established to validate the system works as intended prior to deployment in production.






7. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).
8. Formal change control procedures for all systems must be developed, implemented and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.
  - a. Databases and Software (including in-house or third party developed and commercial off the shelf (COTS):
    1. All software written for or deployed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.
    2. Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data.
    3. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:
      - i. All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or
      - ii. sensitive data is masked or overwritten with fictional information.
    4. Where technically feasible, development software and tools must not be maintained on production systems.
    5. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.
    6. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
    7. Privileged access to production systems by development staff must be restricted.
    8. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.
      - b. Network Systems:
        1. Connections between systems must be authorized by the executive management of all relevant entities and protected by the implementation of appropriate controls.
        2. All connections and their configurations must be documented and the documentation must be reviewed by the information owner and the ISO/designated security representative annually, at a minimum, to assure:
          - i. the business case for the connection is still valid and the connection is still required; and
          - ii. the security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.
        3. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:
          - i. Internet accessible systems and internal systems;
          - ii. systems with high security categorizations (e.g., mission critical, systems containing PII) and other systems; and
          - iii. user and server segments.
        4. Network management must be performed from a secure, dedicated network.
        5. Authentication is required for all users connecting to internal systems.
        6. Network authentication is required for all devices connecting to internal networks.
        7. Only authorized individuals or business units may capture or monitor network traffic.




8. A risk assessment must be performed in consultation with the ISO/designated security representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

Associated Standards: Secure System Development Lifecycle Standard; Secure Coding Standard; Security Logging Standard; Secure Configuration Management Standard

#### 4.12 Collaborative Computing Devices

a. Collaborative computing devices must:

1. prohibit remote activation; and
  2. provide users physically present at the devices with an explicit indication of use.
- b. Must provide simple methods to physically disconnect collaborative computing devices.

#### 4.13 Vulnerability Management

a. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.

b. All systems are subject to periodic penetration testing.

c. Penetration tests are required periodically for all critical environments/systems.

d. Where LEAD College of Management has outsourced a system to another entity or a third party, vulnerability scanning/penetration testing must be coordinated.

e. Scanning/testing and mitigation must be included in third party agreements.

f. The output of the scans/penetration tests will be reviewed in a timely manner by the system owner.

Copies of the scan report/penetration test must be shared with the ISO/designated security representative for evaluation of risk.

g. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.

h. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the ISO/designated security representative. The CISO must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.

i. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested and followed at all times to minimize the possibility of disruption.

Associated Standards: Patch Management Standard; Vulnerability Scanning Standard

#### 4.14 Operations Security

a. All systems and the physical facilities in which they are stored must have documented operating instructions, management processes and formal incident management procedures related to information security matters which define roles and responsibilities of affected individuals who operate or use them.

b. System configurations must follow approved configuration standards.

c. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.

d. Where LEAD College of Management provides a server, application or network service to another entity, operational and management responsibilities must be coordinated by all impacted entities.

e. Host based firewalls must be installed and enabled on all workstations to protect from threats and to restrict access to only that which is needed

f. Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across systems where technically feasible to prevent and detect the introduction of malicious code or other threats.






- g. Controls must be implemented to disable automatic execution of content from removable media.
- h. Controls must be implemented to limit storage of information to authorized locations.
- i. Controls must be in place to allow only approved software to run on a system and prevent execution of all other software.
- j. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.
- k. All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.
- l. Systems which can no longer be supported or patched to current versions must be removed.
- m. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and the Security Logging Standard, and record events to provide evidence and to reconstruct lost or damaged data.
- n. Audit logs recording exceptions and other security-relevant events must be produced, protected and kept consistent with record retention schedules and requirements.
- o. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound and internal network traffic.
- p. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.
- q. Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly. At a se
  1. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).
  2. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.
- r. Backup copies of entity information, software, and system images must be taken regularly in accordance with the entity's defined requirements.
- s. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.
- t. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

Associated Standards: Secure Configuration Management Standard; Security Logging Standard; Cyber Incident Response Standard; Account Management/Access Control Standard

## 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

## 6.0 Definitions of Key Terms

Term	Definition
------	------------

## 7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Entity Address]






**8.0 Revision History**

This standard shall be subject to periodic review to ensure relevancy.

Date Description of Change Reviewer

**9.0 Related Documents**

National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

Internal Revenue Service Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies

