ALLIANCE UNIVERSITY

Private University established in Karnataka State by Act No.34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi

INFORMATION TECHNOLOGY POLICY

Name of the Policy	IT Policy Document
Description of the Policy	Policy on usage of Information Technology Services
Policy Applicable to	Faculty, Staff & Students of the University
Approval Authority	Department of Information Technology Services
Approval Date	October 10, 2022
Responsible Office / Department	Department of Information Technology Services

ALLIANCE UNIVERSITY

Private University established in Karnataka State by Act No.34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi

DEPT. OF INFORMATION TECHNOLOGY SERVICES (ITS)

IT POLICY DOCUMENT

ALLIANCE
UNIVERSITY

DEPT. OF INFORMATION TECHNOLOGY SERVICES (ITS)
AU IT POLICY

Sl. No.	Descriptiion
1	Information Technology (IT) General Policy
2	Data Backup & Recovery Policy
3	Logical Security Access Control - Password Management Policy
4	Security Incident Management Policy
5	E-Mail Policy

ALLIANCE UNIVERSITY

Private University established in Karnataka State by Act No 38 of Year 2010
Recognized by the University Grants Commission (U.G.C.), New Delhi

DEPT. OF INFORMATION TECHNOLOGY SERVICES (ITS)

INFORMATION TECHNOLOGY(IT) GENERAL POLICY DOCUMENT

10/10/2022

Document Title
Information Technology (IT) General Policy Document Document Number: IT-POL-GEN-01 Revision Number: V1.0

Prepared by	Reviewed by	Approved by
Totad		STKawari
Shivakumar Totad Asst. Manager -ITS	Yathish Babu K Manager-IT	Santosh T Kawari CIO

Information Technology (IT) General Policy Document

Reviews follow-up			
Version	**Date**	**Who**	**Item**
Ver 1.0	10-10-2022	Yathish Babu K	Information Technology (IT) General Policy Document

Related Documents			
Document	**Version**	**Writer**	**Description**

Published / Communicated / Posted			
Document	**When**	**Who**	**Audience**
Information Technology (IT) General Policy Document	10-10-2022	Santosh T Kawari CIO	

CONTENTS:

1. INTRODUCTION

The University uses a large amount of information to operate effectively and the majority of this information is in electronic format and held on computers and in our IT systems. It is essential that this information is managed effectively so that it remains secure, accessible to authorized users and its integrity is protected. The IT Security Policy sets standards outlining the way electronic information and IT systems should be managed and operated to ensure the University complies with its obligations in relation to IT Security. The policy sets out how all users of University IT systems and the information they contain must act to ensure these standards and obligations are met.

The policy is divided into several sections. There is a section which contains information applicable to all the workgroup and students and a section which contains information applicable to IT system administrators. All employees and other users of the University's IT systems must read and comply with all sections relevant to them. A glossary of terms is available at the end.

2. SCOPE OF THE POLICY

The IT Security Policy covers all internal University systems and connections to wider networks. It sets out how information contained within or accessible via those IT systems should be handled to ensure it remains secure.

All systems within the University and connections to outside bodies must conform to this policy. The University reserves the right to isolate any IT system or network which represents a potential or actual breach of security; to monitor information sent over its networks; and to deny user access to the universities IT systems.

3. POLICY STATEMENT

The University recognizes the importance of keeping its information and IT systems secure and protected from unauthorized use. Through compliance with this policy, the University will ensure that all university information generated, used and held electronically in IT systems, networks, media and related forms is accurate, secure and available to authorized users for business purposes when needed.

4. RESPONSIBILITIES

This policy applies to all students, employees, including temporary, casual, contract and agency staff, as well as any contractors or service providers acting on behalf of the University.

The Chief Information Officer (CIO) has overall responsibility for ensuring the University complies with this policy. Any questions or concerns about the operation of this policy should be referred in the first instance to Chief Information Officer (CIO).

E-Mail ID: santosh.k@alliance.edu.in

Contact Number:080 4129 9240

This policy is reviewed annually and Recommendations for any amendments should be reported to CIO as part of the review process. Alliance University management will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

5. GENERAL - IT SECURITY POLICY FOR ALL WORKGROUP AND STUDENTS

This policy applies to all the faculty and staff members of Alliance University and other University affiliated institutes / entities. It applies to the use of all IT Systems. These include systems, networks, software's and facilities administered by ITS, as well as those administered by other departments.

Use of IT infrastructure, even when carried out on a privately owned computer that is not managed or maintained by Alliance University, is also governed by this Policy.

Information Technology ("IT"), the vast and growing array of computing and electronic data communications facilities and services, is used daily to create, access, examine, store, and distribute material in multiple media and formats. Information technology plays an integral part in the fulfillment of Alliance University's research, education, administrative, and other roles. Users of Alliance University's IT resources have a responsibility not to abuse those resources and to respect the rights of the members of the University as well as the University itself. This Alliance University IT Policy provides guidelines for the appropriate use of Alliance University's IT resources as well as regulation and enforcement of these policies.

When any use of information technology at the University presents an imminent threat to other users or to the University's technology infrastructure, system administrator may take whatever steps are necessary to isolate the threat, without notice if circumstances so require. This may include changing passwords, locking files, disabling computers, or disconnecting specific devices or entire sub-networks from University.

Computers, network connections, accounts, usernames, authorization codes, and passwords are issued to faculty and staff members to identify them as eligible users of University's information technology. Members are responsible for not sharing their privileges with others, and especially for ensuring that authorization codes and passwords remain confidential. Users of computers connected to the campus network, permanently or temporarily, are responsible for ensuring that unauthorized users do not thereby gain access to the campus network or to licensed resources.

Use of information technology that violates this Policy and rules based on it may result in disciplinary proceedings and, in some cases, in legal action. Unauthorized use of University information technology by Excluded Users may result in police intervention or legal action.

5.1 KEEPING INFORMATION SECURE

Organizational information must always remain secure and must be protected from disclosures to unauthorized parties. Where organizational information is personal data, confidential or commercially sensitive, access to the information must be restricted to those individuals who have a legitimate need for it in order to do their job.

For mobile devices such as tablet computers, PDAs, smartphones etc; the user must ensure the device PIN or password has been set and that the device is set to automatically lock after a short period of inactivity. This will help protect the device against misuse and is an extra safeguard for any personal contact details or any other confidential information held on the device should it fall into the wrong hands; however, this does not replace the need for encryption. Any device without a PIN or password as a minimum-security measure must not be used to hold any organizational information.

Users should note that if a device is lost or damaged, the information stored on it may not be recoverable. These types of devices should therefore never be used to store the only copy of information.

Where encryption is used, decryption passwords must be kept securely and separately. Information which is encrypted cannot be accessed without the encryption password.

5.2 REGULATIONS FOR RESPONSIBLE USE OF INFORMATION TECHNOLOGY: WORKGROUP-SPECIFIC

E-Mail Policy:
At the time of join, HR intimation is sent to IT department to create an official mail id. IT support team will assist the user to configure e-mail client (Microsoft outlook). Privileges to send group mail will be enabled on requirement basis by the system administrator. PST file will be created on the hard disk, where the user can save and personalize e-mails. At the time of relieving, official mail id will be deactivated.

User Login Policy:
User will be provided with a desktop and a telephone extension.
NT login credential will be created, and the user is prompted to change the password at the first login.
User should not share the login credentials with anyone.
Local and National dialing facility will be enabled on authorization from the respective department head. At the time of relieving, the NT login credentials, and telephone facility will be deactivated.

Data Storage Policy:
Cloud storage space for user's data will be made available and it the responsibility of the user to take regular backup of the data onto a cloud storage. ITS helpdesk will only facilitate the user to take backup and shall not be responsible for any data loss due to any circumstances.

GENERAL POLICIES:

1. Workgroup members must abide by the terms of copyright laws, software licensing agreements, and contracts that pertain to the University's computing, information, and communications resources. Reproduction or distribution of copyrighted works, including, but not limited to, images, video, text, audio, or software, without permission of the owner can lead to legal issues.

2. The University's information technology resources are intended to be used to fulfill the University's mission. Use of any of the University's information technology resources for personal profit or gain or for commercial purposes is prohibited.

3. Workgroup members are responsible for the security of their computer accounts, including the changing of passwords on a regular basis. Members are also responsible for all activities that originate from their accounts. Computer accounts are University property and are deactivated according to the University's policies and procedures.

4. Allowing another individual to use one's computer account and/or password is strictly prohibited.

5. Workgroup members may not attempt to access another user's electronic communications, nor may they read, copy, change, or delete another user's files or software without permission of the user.

6. Use of the campus network to gain unauthorized access to any computer account or computer system, to attempt to bypass data protection schemes, to uncover a security loophole, or to mask the identity of a computer account or machine is prohibited.

7. Although the University respects the privacy of an individual's electronic communications, members should be aware that files and mail messages are not guaranteed to be private or secure. Files and messages may be viewed in the course of routine management of computing, telecommunications, and network services. In the event of a security breach, suspected breach, suspected illegal activity, or suspected violation of University policy, files and/or mail may be accessed by authorized personnel.

8. Faculty and Staff members may not deliberately perform an act that will interfere with the normal operations of computers, terminals, peripherals, or networks. This includes, but is not limited to, tampering with any component of a local area network (LAN), Intranet, or wide area network (WAN).

ENFORCEMENT OF POLICY:

Alleged or suspected violations of the IT Policy should be reported to the ITS Help Desk or the concerned University Authorities. All alleged or suspected violations will be reviewed in collaboration with Disciplinary Committee. Abuse of information technology privileges is subject to disciplinary action, which may include the loss of these privileges and other disciplinary sanctions up to and including dismissal. An individual will also be responsible for any financial loss to the University that results from inappropriate use of information technology resources.

5.3 REGULATIONS FOR RESPONSIBLE USE OF INFORMATION TECHNOLOGY: STUDENT-SPECIFIC

1. Students are advised to collect their LAN username and password to access University intranet and internet (www)
   Note: Login credentials to be kept confidential to avoid misuse of the same.

2. Students are advised to register their Laptop/Tab/IPad MAC address for Wi-Fi Access in the Campus. Students are prohibited from accessing Wi-Fi internet in any other devices other than their Laptop/Tab/iPad

3. Student access to internet will be monitored using advanced monitoring tools and hence students are advised to make use of the facility for their Academic and Research purpose only.
   Note: Huge download of data over internet is prohibited and will be monitored.

4. Students will be provided with unique mail id registered to Alliance University domain and hence students are advised to use that mail id for academic purpose only.
   Note: Students are advised not to send anonymous and offensive mails as it will be tracked and may lead to police investigation and legal action.

5. All users are prohibited from posting or writing anonymous/defamatory content against University and University Faculty, Staff and Students.

6. Students must abide by the terms of copyright laws, software licensing agreements, and contracts that pertain to the University's computing, information, and communication resources. Reproduction or distribution of copyrighted works, including, but not limited to, images, video, text, audio, or software, without permission of the owner can lead to legal issues.

7. The University's information technology resources are intended to be used to fulfill the University's mission. Use of any of the University's information technology resources for personal profit or gain or for commercial purposes is prohibited.

8. Students are responsible for the security of their computer accounts, including the changing of passwords on a regular basis. Students are also responsible for all activities that originate from their accounts. Computer accounts are University property and are deactivated according to the University's policies and procedures.

9. Students may not attempt to access another user's electronic communications, nor may they read, copy, change, or delete another user's files or software without permission of the user.

10. Use of the campus network to gain unauthorized access to any computer account or computer system, to attempt to bypass data protection schemes, to uncover a security loophole, or to mask the identity of a computer account or machine is prohibited.

11. Although the University respects the privacy of an individual's electronic communications, students should be aware that files and mail messages are not guaranteed to be private or secure. Files and messages may be viewed in the course of routine management of computing, telecommunications, and network services. In the event of a security breach, suspected breach, suspected illegal activity, or suspected violation of University policy, files and/or mail may be accessed by authorized personnel.

12. Students may not deliberately perform an act that will interfere with the normal operations of computers, terminals, peripherals, or networks. This includes, but is not limited to, tampering with any component of a local area network (LAN), Intranet, or wide area network (WAN).

ENFORCEMENT OF POLICY:

Alleged or suspected violations of the IT Policy should be reported to the ITS Help Desk or the concerned University Authorities. All alleged or suspected violations will be reviewed in collaboration with Disciplinary Committee. Abuse of information technology privileges is subject to disciplinary action, which may include the loss of these privileges and other disciplinary sanctions up to and including dismissal. A student who abuses the University's computing, information, and communications resources may also be subject to civil action and/or criminal prosecution. Alliance University will pursue criminal and civil prosecution of violators when appropriate. Individuals will also be responsible for any financial loss to the University that results from inappropriate use of information technology resources.

5.4 WORKING FROM HOME/REMOTE WORKING

Workgroup members who work from home and use their own home PCs to access the University's computer systems must ensure any personal data or other confidential business information always remains secure. When working away from the campus, users who require access to organizational information must use Remote Access Client. This minimizes the risk of theft or loss of information stored on removable media such as USB sticks. Any data associated with university business that needs to be stored on a laptop or removable media device must be encrypted and stored no longer than necessary. Organizational information must always be stored in an appropriate network location and never on users' personal computers or devices.

Users must note that when using home PCs or other equipment at fixed locations outside the University, they are operating outside the University's IT security perimeter. In these situations, users

must not assume their own PC equipment is protected by the same security measures as standard PC equipment routinely used at the University. Users must be aware that weak security on home PC used for home working could lead to University account passwords becoming known to unauthorized parties, which could lead to security incidents involving University IT systems. It is vital that PCs used for home working are themselves properly secured and it is the responsibility of users to ensure that is so (see list below). Users are responsible for safeguarding the equipment against unauthorized access, misuse, theft, or loss when in their home or in transit, for example on public transport or in their vehicle. Users are also responsible for ensuring that where the equipment is used by others (e.g. family members), no organizational information is accessible by such unauthorized parties.

Users must ensure that all reasonable protection measures are in place and operating where applicable, as follows:

- The computer's local Firewall should be enabled
- Anti-virus software is set to automatically update itself
- Anti-spyware software to provide continuous protection against malicious software being downloaded
- Up to date security patches must be installed for both the operating system and application when they are released by software vendors. Doing so will help protect the equipment against security vulnerabilities that have been identified.
- Wireless networks at home must be properly secured against any intrusion.

Users must always comply with the security requirements of this document and where personal data is being processed, they must also comply with the Data Protection Policy.

Users must not access internal or confidential/sensitive information over unsecured broadband or public wireless networks, including cyber cafes, as these present a security risk. Users should also be aware of the physical environment when working remotely ensuring no one is looking over their shoulder at information on screen.

5.5 PHISHING, VISHING AND SPAM

Information security involves technical security measures but also requires users to ensure they act appropriately to maintain the security of computer systems and the university network. Attacks will be made on these systems and networks by unauthorized parties with the aim of obtaining organizational information or causing damage or disruption to that information or those systems by infecting them with viruses. Users must be aware of such attacks and be able to recognize them in

order to stop them being successful. Attacks may involve phone calls from individuals trying to obtain confidential information by deception or may occur by email. Users must ensure that organizational information is only disclosed by phone to callers who are authorized and entitled to receive that information.

Users must ensure that they do not click on links in spam or phishing emails or emails which appear to be such; attachments to such emails must not be opened. Users must never email their usernames and passwords in response to emails purporting to be from ITS; ITS staff will never ask for users' passwords. Spam and phishing emails are becoming more and more sophisticated and plausible, if in any doubt, do not open the mail and delete it.

If users are in any doubt, they should contact ITS Helpdesk via its.helpdesk@alliance.edu.in / 080 4129 9221

5.6 CLOUD SERVICES

5.6.1 WORKGROUP

Users must follow the University's Data Protection guidelines issued by the ITS department. The only cloud storage service approved for the storage of non-Public categorized information is Microsoft OneDrive for Business, which is part of Office 365. A full security and compliance risk assessment has been undertaken of Microsoft's Online Services by Alliance University.

Users of this service need to be aware of the following;

- University has no direct control over the availability of this cloud service
- Responsibility for the availability, backup and recovery of the service lies with Microsoft.
- Deleted files can be retrieved by the account holder for up to 90 days after which the data may be recoverable by the administrator, however after 180 days it is lost forever.
- Microsoft can and do carryout periodic updates and maintenance, which may result in a loss of service for that period.

It is recommended that Head of the Department with an approval of CIO shall take the back up of important/critical data in an external drive, and in an emergency deleted files can be retrieved within hours.

5.6.2 STUDENTS

The only cloud storage service recommended by ITS is Microsoft's OneDrive for Business, which is part of Office 365.

Users of this service need to be aware of the following;

- University has no direct control over the availability of this cloud service
- Responsibility for the availability, backup and recovery of the service lies with Microsoft.
- Deleted files can be retrieved by the account holder for up to 90 days after which the data may be recoverable by the administrator, however after 180 days it is lost forever.
- Microsoft can and do carryout periodic updates and maintenance, which may result in a loss of service for that period.

It is recommended that students shall take the back up of important/critical data in an external drive in addition to the storing data in OneDrive.

For further advice, contact ITS Helpdesk via its.helpdesk@alliance.edu.in / 080 4129 9221

5.7 SECURITY BREACHES

All users must report all actual or suspected security breaches to the Information Security Team in ITS department (its.helpdesk@alliance.edu.in / 080 4129 9221) as soon as they become aware of it, whether they have caused the breach or they are informed of the breach by another party. ITS will ensure that any security breaches reported to them are acted upon promptly and will keep appropriate records and documentation. Corrective actions taken and other resolutions will be documented and monitored. In cases where an incident involves personal data, it must also be reported to the CIO without delay, following which it will be managed and reported in line with the University Information Governance Incident guidelines.

5.8 DESTRUCTION AND DISPOSAL OF EQUIPMENT

Any equipment or media used to store personal data or other organizational information must be disposed of securely, users should log a request with the ITS Support team who will refer them to the relevant technician. No equipment or media containing or used to access organizational information must be disposed of or sent for resale without ensuring that all information has been removed and is irrecoverable. Any third parties who provide a destruction and disposal service under contract on behalf of the University must follow the agreed contractual procedures for removal of information. It must be noted that even though a third party may be contracted, the University is still ultimately responsible for the data and can be prosecuted should the Data Protection guidelines be breached.

5.9 ID CARDS AND ACCESS CONTROL CARDS

Lost or misplaced university identity cards present a security risk because the information they contain may, in some circumstances, allow an unauthorized user in possession of the card to gain access to live accounts. Consequently, it can also mean that in some cases, organizational information or other significant parts of computer systems are at risk. The loss of cards used for controlling access to buildings or secure rooms can potentially lead to a breach of physical security.

To guard against such events, if cards are lost or stolen, users must report its loss to the place of issue at the earliest opportunity but no later than 48 hours. If the card is used to access and administer university IT systems, then the loss must be reported immediately to the ITS team. Administrators handling a report of a lost card must immediately disable the card and revoke any access privileges associated with it on the relevant systems. Users must follow relevant procedures for a replacement card to be issued.

When a lost card is found, the card must be handed in to the place indicated on it. The relevant user should be informed that the card has been found. If the loss has not already been reported, the user should also attend the relevant place for a new card to be issued. The lost card should never be returned to users; a new one must always be issued. The lost card must be disabled on the relevant systems for the reasons outlined above. To help protect the personal information held on such cards, the old card must be physically destroyed and not disposed of intact to ensure information contained in it is not accessible after it has been disposed of.

5.10 COPYRIGHT

Copyrighted and licensed software must not be duplicated, removed or added by users unless it is explicitly stated that this is acceptable. Information about copyright is available to staff on the intranet. All copyright requirements must be complied with and declarations must be signed where appropriate.

The University's IT systems and network infrastructure, including wireless and Network-Lite must not be used for the downloading or streaming of copyrighted materials including but not limited to video and audio files, without the written consent of the owner or copyright-holder.

5.11 USE OF SOFTWARE

Copyrighted and licensed software may not be copied or distributed by users in contravention of the licensing agreement. Users are not permitted to trial software, for example from a removable disk on university computers, and are not permitted to modify the operating system either manually or by downloading applications such as screensavers, themes etc.

Personal use of peer-to-peer networking and file sharing applications is not permitted on any of the University's systems. These applications use University resources for non-University purposes, they increase the risk of virus infection and spyware which compromise privacy and security and they involve legal risks regarding the storage of copyrighted material.

It is University policy that no member of the Alliance University community engage in any activity that violates central, state, or local laws with respect to intellectual property rights; the terms of software license agreements; or other University policies pertaining to computer software, for any computer software owned by or licensed to the University and computer systems or hardware owned or operated by the University, faculty, staff, and students;

- Must abide by all terms of the software license agreement.
- Must be aware that ALL computer software is protected by copyright unless it is explicitly labelled as PUBLIC DOMAIN.
- Must not copy software for any purpose outside those allowed in that software's license agreement.
- Must not make software available for others to use or copy in violation of that software's license agreement.
- Must not accept unlicensed software from any third party.
- Must not install, nor direct others to install, illegal copies of computer software or unlicensed software onto any University-owned or operated computer system. It is recommended that individual University colleges/schools/departments units conduct and maintain periodi

reviews of its computer systems for software installations to help ensure compliance with licensing agreements, copyright regulations, and University policy.

6. NETWORK MANAGEMENT CYBER SECURITY AND /DATA PRIVACY PROTECTION CONTROLS

6.1 PROTECTION FOR THE EXTERNAL NETWORK LINK

The external network link is managed by ITS team to provide security, control and auditing of usage. Any computer systems using the external network link must have approval from ITS team to do so. The administrators of such systems must ensure compliance with the security requirements of this document. Any broadband/ISDN/leased circuit access must not be connected to the main University networks but must connect through an ITS-managed or authorized firewall to avoid compromising security or must be completely standalone.

Data privacy aims to enable the analysis and sharing of personal and confidential data, which are being collected and stored by organizations and individuals.

Cybersecurity covers processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction.

Unlike private enterprises, colleges and universities operate on an open-campus model designed to encourage fluid information exchange. As such, the communities and data systems are often very porous by design, allowing cybercriminals more opportunities and entry points to breach the systems.

6.2 USER AUTHORISATION

The University will ensure that all computer system users are formally authorized to use the network and an audit trail of authorization is maintained. Students are authorized through the enrolment process as being fee-paying students of the University. Staff are authorized by Human Resources and their department Heads, with sensitive data access being specifically requested. External users are authorized by ITS team and may be given access to computer systems where appropriate.

6.3 HARDWARE AUTHORISATION

ITS team will maintain an inventory of authorized network equipment including network components, servers and workstations. Unauthorized hardware will be removed.

6.4 CONTROLS ON PHYSICAL ACCESS TO COMPUTER EQUIPMENT

Physical access to the servers and related components will be limited to authorized personnel. The servers, back-up facilities, UPS, network hubs, etc. will be installed in locked areas which are only normally accessible to the computer system administrators and relevant technical support staff. Rooms used to house server and other sensitive system equipment will be kept locked and access to them restricted and monitored. Where workstations are located in public areas or areas that can be

accessed by the public or students, consideration will be given to securing workstations and printers to desks and installing CCTV monitoring equipment.

6.5 PROHIBITION OF NON-STANDARD HARDWARE AND SOFTWARE

All devices connected to the university network are to be standard hardware managed by ITS team. Any non-standard hardware and software must be hosted on an existing non-university network behind firewall protection. Any exception to the above is by the prior express permission from the CIO or nominee. This is subject to a security risk assessment which must be made by suitably qualified ITS staff. The CIO or nominee may refuse and reasons for refusal are various, including but not limited to the following:

- In the judgment of ITS, the equipment might in any way interfere with, or be a risk to, the correct functioning of the university network or any approved systems.
- The equipment has inadequate protection against infection by malicious software.
- The equipment is not properly secured against unauthorized access and misuse.

6.6 WORKSTATION CLIENT SOFTWARE PROTECTION

ITS will deploy security-related software patches and updates to the university computer systems following the guidance of the ITS system patching and update policies. The administrators of non-university systems will be responsible for the deployment of the relevant security related patches for those systems.

6.7 PROTECTION OF WEB-BASED SERVICES

Certain web-based services, for example access to University databases containing personal or confidential information, will have extra protection against eavesdropping on the Internet. SSL (Secure Sockets Layer) will be used to establish a secure connection between the client and server for transmission of information in encrypted form.

6.8 RISK ANALYSIS

Responsibility for conducting periodic risk analysis and security assessments will be formally assigned. The owner of the computer system mainly ITS administrator is responsible for assigning responsibility for periodic risk analysis and security assessments of the computer systems. Risk analysis and security assessments will be conducted during the system design stages and at any other times when changes are made to the system design and/or components. Such analysis/assessments will measure the network's vulnerability to:

- Inadvertent error or improper disclosure of information.
- Fraud or theft.
- Financial loss.
- Harm to individuals from infringement of privacy rights.
- Loss of proprietary information and harm to organizational activity.

6.9 PHYSICAL SECURITY

Physical security of the computer systems, including central servers and workstations, is a critical aspect of IT security. To maintain protection against intrusions, it is important that access to critical computer system components (such as the servers) is restricted to a small number of authorized individuals. Other considerations will include protection of equipment against theft, fire, and electrical hazards.

The university computer systems will be located in locked rooms to which access is restricted to authorized ITS staff. The university computer systems will have adequate backup power for critical components. Wiring closets housing network equipment will always be kept locked with access restricted to authorized ITS staff and approved third party companies e.g. data and electrical installers. Workstations in public access areas will be provided with appropriate physical security and be monitored by CCTV surveillance equipment where appropriate. Visitors to restricted areas should be supervised by authorized ITS staff/Security administration.

6.10 VIRUS PROTECTION

A virus infection is an annoyance to users of a personal computer and in some instances, a virus may end up costing the user a lot of time through destruction of information or by preventing the user from being able to access the data stored on a hard drive. Increasingly likely is the possibility of a personal computer being infected but showing no outward sign. The compromised personal computer may behave in a way that impacts on its local network or may have effects on external sites by hijacking normal communication mechanisms for the virus' propagation or other unwelcome activities.

PROTECTION MEASURES

Anti-virus software's and clean-up programs are installed on the system file servers and workstation clients. User files are scanned on writing to server system to detect viruses. The workstation client ant-virus software is configured to scan on writing files to the local hard drives and any other local storage including secondary hard drives, CD/DVD drives and USB flash drives will be scanned on both reading and writing where technically possible.

The anti-virus software will be updated regularly in order that it may detect new viruses. Virus outbreaks will be monitored to determine if changed action is required because of a particular or new virus.

USER AWARENESS OF VIRUS ISSUES

Users will be warned that virus scanners are not fool-proof and are largely reactive to new viruses, leaving a window of opportunity for new viruses before they are detected and incorporated in a scanner. Users will always be careful to verify the source of computer-based information. If a file is discovered to be infected the onus is on the user to notify all sources and destinations of the file to prevent further spread (and maintain goodwill). Users must be particularly careful when distributing files, especially by email, to avoid spreading viruses. Unnecessary use of email attachments will be discouraged.

7. POWER BACK-UP FOR IT AND IT ENABLED SYSTEM

Uninterruptible Power Supply (UPS) systems provide continuity of service for IT and IT Enabled systems in the event of power failure and so enable the University to deal with several risks associated with power failure. The High capacity Generator System will switch on automatically in the event of power failure which has power backup capacity for whole University campus including IT and non-IT facilities. The University facility department is responsible for managing and maintaining the UPS and Generator systems. The facility department is advised to implement systems that:

- Ensure dedicated UPS systems for IT Data Center and Hub Rooms and centralized UPS systems for individual building blocks.
- Ensure UPS's and Generator system are recorded on a register and regular inspections as per manufacturer's instructions are undertaken with records kept.
- Ensure all UPS and Generator systems are under Annual Maintenance Contract (AMC) with OEM's with defined SLA's.

- UPS systems at the end of their design battery life must be disposed of as E waste through IT Services.
- Any maintenance of UPS and Generator systems shall be carried out by competent Electrical Engineers.
- All UPS systems greater than 1kVA and Generator systems should be considered in the fire risk assessment.

8. SERVICE LEVEL AGREEMENT (SLA)

A Service Level Agreement (SLA) is a service-based commitment between Information Technology Services (the service provider) and the University procuring the technology service.

Each SLA includes:

- A description of the service
- Service term and costs
- Service performance, support and service level targets
- Service provider and customer responsibilities
- Technical contacts
- Approval signatures
- A single SLA may cover multiple IT services

Below you will find a list of the ITS services available to include in Service Level Agreements.

- Software Licenses and subscription
- Firewall & Endpoint Security Services
- Internet Service Provider
- Service Level Contract for Network Equipment's
- Virtual Server Hosting
- Service Agreement for printers

9. IT ACCESSORIES MANAGEMENT

An IT spare accessory is a replacement unit that is kept in an ITS inventory and used for the repair or replacement of failed units.

At Alliance University, planning is done during the time of procurement, keeping in mind the accessories required for replacement during hardware failure be it laptop/computer/printer/server/ network component.

Below are the best practices:

- When financially possible, computer systems will be replaced within the fiscal year in which they are determined to be end-of-life.
- A computer will be refreshed on a one-to-one basis only (ex: a desktop replaces a desktop; a laptop replaces a laptop).
- Any old system must be returned to the ITS department for disposal. Special consideration will be made for end-of-life machines that do not require network connectivity and ITS support for their intended function.
- In all cases, if a Mac-based system is chosen, the employee should have a valid reason for doing so (job function or applications require it, etc.) as they are generally more expensive to purchase and maintain.
- Any computers or accessories that stop functioning not due to misuse will be replaced by the ITS department.
- Any computers or accessories that are lost or stolen may be replaced by department funds. These items will not be refreshed until replaced.
- Any computers or accessories that are damaged beyond normal wear and tear may be replaced via departmental funds.
- Any Printer, Server and Network component reported faulty shall be replaced with minimal downtime.

10. IT TECHNICAL SUPPORT AND HELPDESK

IT Technical Support in University refers to the experience students and stakeholders have when interacting with their school or colleges.

To deliver a seamless experience and provide value to all their customers, IT Technical support/Helpdesk need to be:

– **Be responsive:** reply to incoming queries quickly and efficiently

– **Be available:** ensure everyone knows where they can find the information they need.

– **Be service-orientated:** seek feedback and deliver on requests from students, staff/faculty and parents.

To back up its Technology Enabled and Online teaching and Learning Services, Alliance University has a highly qualified team of professionals handling the help desk and technical support. These servi[illegible] are available 24 x 7 to help resolve issues that may arise during the complete enrolment and on-rolls cycle.

Log Support via Phone:

The students and faculty/staff can call dedicated ITS Help Desk number. The support Engineers will address the user request on call or by remotely connecting the user system if required.

Log Support via Email:

The students and faculty/staff can email support request to dedicated ITS Help Desk Email id with necessary details. The support Engineers will address the user request on call or by remotely connecting the user system.

Online Support Request:

The student and faculty/staff shall visit ERP/student portal to submit any IT support ticket. The users can access this website from any computer or cell phone that has an Internet connection.

The IT support is categorized into four divisions:

DESKTOP SUPPORT: The dedicated-on call support is available for students and faculty/staff to resolve their system level hardware or software issues. The Dedicated Desktop Support Engineers will address the user issue on call only by immediately connecting the user system remotely if required. The support Engineer will visit the user desk physically also if required.

SERVER SUPPORT: The dedicated server support Engineers are available on call or remote support to address the server related issues of students and faculty/staff.

NETWORK SUPPORT: The dedicated-on call support is available for students and faculty/staff to resolve their Network issues which may include LAN or Wi-Fi. The Dedicated System Administrator or Network Engineer will address the user issue immediately by checking the network systems. The support Engineer will visit the user desk physically also if required.

APPLICATION SUPPORT: The dedicated-on call support is available for students and faculty/staff to resolve their application level issues including ERP, LMS and other standalone applications used in the University. The Dedicated Support Engineers will address the user issue on call only by immediately connecting the user system remotely if required. The support Engineer will visit the user desk physically also if required. The issues related to use of technology or software designed and developed by Alliance University are addressed by the technical support representatives.

The help desk representatives are trained by University to be customer friendly, patient, empathetic, courteous and have relevant subject knowledge. An efficient and well-structured tracking mechanism to is also in place to keep a tab on all complaints registered with the help desk and ensure their quick and satisfactory redressal.

End User Support Services provides a wide variety of technical support to students, faculty and staff to enhance learning through the use of technology.

11. GLOSSARY OF TERMS

User	→	The individual who uses the computer systems
Computer systems	→	All campus networks, servers, workstations and network access devices
Organisational information	→	Information relating to the running of the University. This may be personal information about students, staff, external customers and contractors; information shared with the University by its business and research partners; or corporate information which is confidential or commercially sensitive.
Personal data	→	Data relating to a living individual who can be identified from that data (or from that data and other information in our possession or likely to come into our possession). Personal data can be factual (such as name, address, date of birth) or it can be an opinion (such as aspects of an employment reference). Information can be personal data without including a person's name.
Security incident/breach/violation	→	Any incident where the security of the computer system, corporate network or organisational information is compromised e.g. due to unauthorised access or disclosure.
Cloud services	→	Online storage areas hosted by organisations external to their network where information can be stored and accessed via an individual user account e.g. Google Cloud.
University network	→	All infrastructure intended to support the University IT requirements.
Chief Information Officer (CIO)	→	It is job title given to the most senior executive in an enterprise who works with IT and computer systems, in order to support enterprise goals.

ALLIANCE UNIVERSITY

Private University established in Karnataka State by Act No 34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi

DEPT. OF INFORMATION TECHNOLOGY SERVICES (ITS)

Data Backup and Recovery Policy

10/10/2022

Document Title
Data Backup and Recovery Policy Document Number: IT-POL-DBR-01 Revision Number: V1.0

Prepared by	Reviewed by	Approved by
Totad		
Shivakumar Totad Asst. Manager -ITS	Yathish Babu K Manager-IT	Santosh T Kawari CIO

Data Backup and Recovery Policy

Reviews follow-up			
Version	**Date**	**Who**	**Item**
Ver 1.0	10-10-2022	Yathish Babu K	Data Backup and Recovery Policy

Related Documents			
Document	**Version**	**Writer**	**Description**

Published / Communicated / Posted			
Document	**When**	**Who**	**Audience**
Data Backup and Recovery Policy	10-10-2022	Santosh T Kawari CIO	

Contents

1 Overview

To ensure reliable availability of data, Alliance University recognizes the need for structured, highly formalized data backup and restoration procedures. Alliance University understands the impact to business of non-availability or discontinuity of availability of data and the associated business risks.

To withstand, recover from, and lessen the effects of any disruptive event compromising the availability of data such as hardware failures, security risks and physical security, Alliance University has setup a comprehensive data backup and recovery policy covering all digital assets of the organization to ensure data availability in the shortest possible time.

1.1 Scope

The scope of this policy includes all information technology systems, software, databases, applications and network resources needed by the University to perform its day-to-day operations.

1.2 Audiences:

IT Team, Assessment Team, Alliance University Team, Vendors and contractors, HR, Finance

1.3 Responsibilities and actors

Users are responsible for the complete application of the following points if they are impacted. IT Staff is responsible for the correct implementation of the following points:

2 Policy

All data backup and recovery tasks for the University must be managed by the information technology (IT) department. The IT department must receive the demands from all departments, including Finance and Accounting, Human Resources, for data backup, protection, and recovery.

The IT department must make sure that data is backed up and securely stored, with the ability to access and restore the data as quickly and securely as possible while adhering to Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of the applications / systems. Procedures for data backup and recovery must be created, carried out, and periodically tested by the IT department. Additionally, the IT division's operations must adhere to the necessary industry standards for data backup.

2.1 Common use cases

Regardless of the IT infrastructure provider, there is the potential for failures to impact business workload. Therefore, Alliance University must take steps to implement resiliency to make the workload reliable. The University needs protection against threats like ransomware. Proper data protection allows the business to meet the demands of numerous use cases such as:

2.1.1 Business continuity

With backup policies, an organization can protect all its data and bring business back to life following unpredictable disruptions.

2.1.2 Data protection

Without proper protection, the data remains susceptible to potential loss and corruption. A correctly implemented backup policy preserves the data integrity and provides usable copies of lost or corrupted data.

2.1.3 Disaster recovery

It is accepted that all businesses and IT environments will face unexpected events that could cause data loss, corruption, or disruption of IT operations. Using a sound backup policy ensures recovery and return to normal with reduced risks due to unplanned disruptions.

2.1.4 Regulatory compliance

Backup policy can be used to respond to audits and demonstrate compliance with data regulations through proper documentation and reporting.

2.2 Recovery time objective (RTO) and Recovery point objective (RPO)

Alliance University must determine the recovery time objective (RTO)* and recovery point objective (RPO)* for each of its IT servers and applications.

The time it takes to recover data should be considered when choosing a backup strategy. The complexity of the data reproduction mechanism or the type of backup (in the case of a backup strategy) will determine how long it takes to recover data. Such time requirements ought to be covered by the workload's RTO.

2.3 Identify data for backup

A formal risk assessment (RA) and business impact analysis (BIA) shall be undertaken to determine the requirements for all data backup and recovery plans; RAs and BIAs shall be updated at least annually to ensure they are in alignment with the business and its technology requirements.

Determine and categorize the data sources according to their criticality using RA and BIA. Next, develop a backup and restoration plan based on the RPO for data recovery. This tactic entails either having a backup of these data sources or the capability of reproducing data from other sources. When data loss occurs, the backup and recovery plan used should allow for data recovery or reproduction within the specified RPO and RTO.

2.4 Data backup and recovery plan

Alliance University must develop comprehensive data backup and recovery plans in accordance with good data backup and recovery management practices as defined by this policy. The data backup and recovery plan for each system must be formally documented and approved by the system and data owners.

Data backup and recovery plan should include:

a) Planning and design of data backup and recovery activities.
b) Identification of data backup teams, defining their roles and responsibilities and ensuring they are properly trained and prepared to respond to an incident.
c) Planning, design and documentation of data backup and recovery plans.

d) Scheduling of updates to data backup and recovery business impact analysis.
e) Scheduling of updates to data backup and recovery risk assessments.
f) Planning and delivery of awareness and training activities for employees and data backup team members.
g) Planning and design of incident response activities associated with data backup and recovery.
h) Planning and execution of data backup and recovery plan exercises.
i) Designing and implementing a data backup and recovery program/plan maintenance activity to ensure that plans are up to date and ready for use.
j) Preparing for management review and auditing of data backup and recovery plan(s)
k) Planning and implementation of continuous improvement activities for the data backup and recovery program and plan(s).

2.5 Data backup and recovery plan review

Data backup and recovery plans must be periodically tested in a suitable environment to ensure that the systems, networks, databases, applications and other infrastructure elements can be recovered and returned to a business as usual (BAU) status in emergency situations and that Alliance University management, and employees understand how the plans are to be executed as well as their roles and responsibilities.

All concerned employees must be made aware of the data backup and recovery plans and their own roles and responsibilities during an incident.

2.6 General backup and recovery guidelines

The following holds for both physical and cloud infrastructure:

a) Backups of Critical Users Laptops, application servers, database server and/or file servers must be taken (PST / OST files may be excluded).
b) No User should be permitted to create or delete any system files or folders.
c) All production system-level folders and files must be part of the Alliance University backup plan.
d) No User is allowed to store any unproductive software / files (Ex. Games, music files etc.) which are not related to business objectives of Alliance University. ITS team of Alliance University shall have all rights to delete all these kinds of material from the System and backup of these files will be taken.
e) All Backup Activities must comply with the guidelines described in this policy.
f) There should be periodic testing of backup media at both on-site and off-site locations (at least once a year) to ensure that backup is in useable condition for recovery and that their contents are as documented. Backup media found to be unreadable must be reported to the CIO.

2.7 Specific guidelines and instructions

2.7.1 On premises

a) Backup should contain documents files of users, production databases, production data kept outside databases, SAS, TFS, File Servers, etc. for recovery.
b) Automated backup should be taken of all HOD and critical users' data using tools.
c) The proper backup and the confirmation of the backup is the responsibility of the engineer who is taking the backup. Backup logs shall be maintained.

d) Disk movement from the University premises to the offsite location should be informed to the IT Manager before leaving the University premises and only IT manager is responsible for proper exchange of tapes between the University Campus premises and the offsite location, if any.
e) In the case of any exception (ex. Suspected leakage of information from the Backup) the IT manager should inform immediately to the CIO / IT Head.
f) Backup should be done in a manner of Disk to Disk to Tape for ease and Quick process.
g) Backup of web server files shall be kept in version control system and backup of Version control system shall be done regularly.
h) Backup of the SQL server database shall be done in sync with database administrator/ Manager.
i) The System Administrator should instruct laptop users to make folders in a structured manner or ask them to restructure the same.
j) Copies of backup files and documentation must always be kept off-site in a secure location.
k) Security of backup storage media must be maintained in compliance with the physical security / Environmental controls standards.
l) All movements of backup media must be monitored and logged. Authorized staff may carry out the deposit and withdrawal of backup media from storage locations only.
m) Copies of backup files moved to or from off-site storage locations must be provided with defined and agreed levels of security during transportation.

2.7.2 Cloud infrastructure

The cloud infrastructure management should follow stated terms and guidelines:

a) Regular Backups of Database for University production database accounts should be taken.
b) Change or service requests should be subjected to on Demand AMI backups for EC2 instances.
c) For all databases full, differential and log backup should be taken using Native Backup tools.
d) All Backups exception logs to be uploaded on AWS S3 buckets by next day.
e) While storing and managing backups complete data security should be ensured and effective measures should be taken to ensure there is no data loss/data leakage/unauthorized access/accidental deletion, etc.
f) All applications, APIs and website code must be version controlled using a best in class, SAAS based version control system.

2.8 Periodicity of backups for on premises

2.8.1 Daily

a) Backups which are scheduled for daily basis should start from the specified time and must inform the users 1 day prior to the down time (if any).
b) Backup should be done in the Disk to Disk.
c) Disks must carry a systematic and standard format (formed by IT Manager) of written slip which should stick on the disks accordingly and it is the responsibility of the engineer who is available at the completion of the backup.

2.8.2 Weekly

a) Backup which are scheduled for Weekly basis should start from the specified time and must inform the users 1 day prior to the down time (if any).
b) Backup should be done in the Disk to Disk to NAS manner.

c) Backup disks which are going off location should contain the encrypted form of data for security reasons.
d) Disks must carry a systematic and standard format of written slip which should stick on the disks accordingly and it is the responsibility of the engineer who is available at the completion of the backup.

Restoration Check

a) Restoration checks shall be done regularly of random backups and logs of restoration activity must be maintained.
b) Restoration, done on need basis, shall be checked by the owner of the data as per restoration request for the confirmation of the data integrity.

2.8.3 Monthly

a) Monthly backups shall be done regularly.
b) Backup which are scheduled for monthly basis should start from the specified time and date and must inform the users 1 day prior to the down time (if any).
c) Backup should be done in the Disk to Disk to NAS manner.
d) Tapes must carry a systematic and standard format of written slip which should stick on the tapes accordingly responsibility is of the engineer who is available at the completion of the backup.

2.8.4 Periodicity of backups for on premises

Backup plans on cloud should be scheduled based on the RPO and RTO mandate of Alliance University for cloud hosted applications, databases, servers and services.

Restoration check

a) Restoration checks shall be done regularly of random backups and logs maintained.
b) Restoration, done on a need basis, shall be checked by the owner of the data as per restoration request for the confirmation of the data integrity.

2.9 Securely backup

Backups of both on premises and on cloud infrastructure must be access controlled and access should be granted in accordance with the access control policy of Alliance University.

2.9.1 Encryption

Backups should be stored encrypted on the tape or hard drives.

2.10 Retention period

The retention period of backup must be in accordance with relevant regulatory requirements. This must be documented in operations procedures. Business Owner should define regulatory requirements.

2.11 Third Party

Where a third party has been authorized to store backup media, a service level agreement (SLA) should be defined and documented, and in compliance with the IS Security Standards.

2.12 Automated backups

Automated backup functions within software packages should be used where applicable.

2.13 Backup after change

All critical systems backup must also be carried out immediately before and after the deployment of any upgrade, change done to a system or/and application.

2.14 Restoration

2.14.1Authorization

Authorization to restore data from backup media that would overwrite existing production data must be obtained from Data Owners in writing and in compliance with the BCP and DR plans.

2.14.2Recovery and restart procedure

Recovery and restart procedures must be established and briefed to relevant parties for each critical system and/or application. The document must be easily accessible to the authorized parties.

2.14.3Support material

Source documents, reports and backup media necessary for reconstruction of a system must be identified, well documented and appropriately placed for easy access by the intended parties in the event of a recovery execution.

2.14.4 Recovery point objective (RPO)*

Restoration of the current configuration must be within agreed recovery point scales as mentioned in the backup and recovery plans.

2.14.5 Recovery time objective (RTO)*

Restoration of the current configuration must be within agreed recovery time scales as mentioned in the backup and recovery plans.

2.15 Exception

In situations where data backup and recovery activities do not comply with this policy, the IT data backup team will prepare a report stating the reason(s) for non-compliance and present it to IT management for resolution.

In case the exception cannot be mitigated to the extent of eliminating the underlying risk, the exception must be escalated to the business management to obtain explicit approval for the exception.

2.16 Reporting

Proper reporting is a very important part of the Backup procedure system will follow the instructions given below:

a) The backup engineer shall maintain records of tape labels (containing data information–data month, etc).

b) The Backup engineer should inform the users for the down time of the database during the backup activity, if required, before one day.
c) The Backup Engineer shall regularly review backup logs of both on premises and on cloud.
d) Each Owner of database system should confirm the quality of backup to the IT whenever restorations are done.
e) Backup Engineer should check the place of storing disks frequently and ensure that the disks are kept secure and the place is environment friendly.
f) Backup Engineer should analyze the capacity of databases with respect to the number of disks and should raise request before at least 15 days for the same.
g) The Backup disks should be kept in a waterproof and fireproof place and the physical security of the same shall be maintained.
h) For Cloud infra the automated mail alert for DB backup failures and success reports shall be configured and maintained.

3 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4 Review process

This document has to be reviewed yearly.
The review has to be performed by the owner of the document.
The final document has to be reviewed by the Manager-ITS and approved by the CIO.

5 Communication process

This document can only be communicated when approved by the concerned authority.

5.1 Glossary

5.1.1 Recovery Time Objective (RTO):

The recovery time objective (RTO) is the amount of real time a business has to restore its processes at an acceptable service level after a disaster to avoid intolerable consequences associated with the disruption.

5.1.2 Recovery Point Objective (RPO):

A Recovery Point Objective, or RPO, is the maximum amount of data that can be lost before causing detrimental harm to the organization. RPO indicates the data loss tolerance of a business process or an organization in general.

5.2 Advice

This document is a general policy and covers information security concepts at a high level, defines these concepts, describes why they are important. The technical documents describe how to

implement this policy locally. If necessary, you must write a procedural document for applying this policy.

ALLIANCE UNIVERSITY

Private University established in Karnataka State by Act. No. 34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi

DEPT. OF INFORMATION TECHNOLOGY SERVICES (ITS)

Logical Security Access Control Password Management Policy

10/10/2023

Document Title
Logical Security Access Control - Password Management Policy Document Number: IT-POL-PM-01 Revision Number: V1.0

Prepared by	Reviewed by	Approved by
Totad		STKawari
Shivakumar Totad Asst. Manager -ITS	Yathish Babu K Manager-IT	Santosh T Kawari CIO

Logical Security Access Control - Password Management Policy

Reviews follow-up			
Version	**Date**	**Who**	**Item**
Ver 1.0	10-10-2022	Yathish Babu K	Logical Security Access Control - Password Management Policy

Related Documents			
Document	**Version**	**Writer**	**Description**

Published / Communicated / Posted			
Document	**When**	**Who**	**Audience**
Logical Security Access Control - Password Management Policy	10-10-2022	Santosh T Kawari CIO	

1 Overview

Password is an important aspect of asset security – It is the front line of protection for user accounts. A poorly chosen password may result in the compromise of Alliance University's entire network and asset. As such, all Alliance University employees (including contractors and vendors with access to Alliance University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1.1 Scope

Entire organization of Alliance University

1.2 Audiences:

IT Team, HR Department, Assessment Team, Alliance University Team, Third Party Contractors

1.3 Responsibilities and actors

Users are responsible for the complete application of the following points if they are impacted. IT Staff is responsible for the correct implementation of the following points:

2 Policy

2.1 Appropriate controls

Audit and Tools to control the compliance with this policy.

2.2 Password and user-id construction

2.2.1 Minimum password length

The length of passwords must always be checked automatically at the time that users construct or select them. All Users passwords must have at least eight (8) characters and all Administrators passwords must have at least fourteen (14) characters. The password guidelines are given below:

- Passwords are case-sensitive.
- Passwords must be between 8 and 64 characters in length.
- Passwords must contain at least one character from each of the following four categories:
  - Lowercase letters (a-z)
  - Uppercase letters (A-Z)
  - Numbers (0-9)
- Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- The last three passwords cannot be reused.

2.2.2 Difficult-to-guess passwords required

All user-chosen passwords for computers and networks must be difficult to guess. Words in a dictionary, derivatives of user-IDs, and common character sequences such as "123456" must not be employed. Likewise, personal details such as spouse's name, automobile license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters.

User-chosen passwords must also not be any part of speech. For example, proper names, geographical locations, common acronyms, and slang must not be employed.

2.2.3 Multi-factor authentication

In all applications which support multi-factor authentication, the multi-factor authentication must be enabled and engaged for authentication and authorization of the users.

2.2.4 User-chosen passwords must not be reused

Users must not construct passwords which are identical or substantially similar to passwords that they had previously employed.

2.2.5 Previous password history file

On all multi-user machines, system software or locally developed software must be used to maintain an encrypted history of previous fixed passwords. This history file must be employed to prevent users from reusing fixed passwords. The history file must minimally contain the last five (5) passwords for each user-ID.

2.3 Design of password system user interface

2.3.1 Display, storage and printing of passwords

The display, storage and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.

2.3.2 Periodic forced password changes

All users must be automatically forced to change their passwords at least once every ninety (90) days.
All Administrators must be automatically forced to change their passwords at least once every sixty (60) days.

2.3.3 Assignment of expired passwords

The initial passwords issued by a security administrator must be valid only for the involved user's first on-line session. At that time, the user must be forced to choose another password before any other work can be done.

2.3.4 Initial one-time passwords transmitted to remote users by authorized means

The user name / user ID and password should not be sent through the same channel of communication. For example, if the user name is shared on mail, the password should be shared through SMS/WhatsApp/Signed courier etc.

The initial one-time password for a new remote user must be sent via a communications channel other than the channel used to log-in to Alliance University Group systems. Authorized means of transmission include courier service requiring a signature, SMS, WhatsApp, and in-person appearance at a trusted intermediary's office along with the provision of picture identification. All

information can be provided to his/her management, the IT contact, a key user under condition that these persons have been previously identified.

2.3.5 Limit on consecutive unsuccessful attempts to enter a password

To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three (3) unsuccessful attempts to enter a password, the involved user-ID must be either: (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than twenty minutes (20 Min), or (c) if dial-up or other external network connections are involved, disconnected. The remedial action to be dependent on the criticality of the business function and asset involved.

2.3.6 Single sign-on policy

Users must be asked for only one (1) user-ID and password combination at the time they reach the network and/or destination computer system. User identity related information must then be passed all digital assets, database management systems, and applications authorized for the user, automatically using the single sign-on functionality.

2.4 Scheduled *password changes communicated*

All password resets or changes must be promptly communicated to all the stakeholders by regular e-mail to confirm and ensure their access to the affected systems. Any change in the password without proper email communication should be deemed unauthorized.

2.4.1 Protection of passwords sent through the mail

If sent by regular mail or similar physical distribution systems, passwords must be sent separately from user-IDs. These mailings must have no markings indicating the nature of the enclosure. Passwords must also be concealed inside an opaque envelope that will readily reveal tampering.

2.4.2 Storage of passwords in readable form

Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, code and configuration files, in computers with or without access control, or in other locations where unauthorized persons might discover or use them.

2.4.3 Encryption of passwords

Passwords must always be encrypted when held in storage for any significant period of time or when transmitted over networks. This will prevent them from being disclosed to wiretappers, technical staff who are reading systems logs, and other unauthorized parties. A competent password management software should be used for storage and transmission of passwords.

2.4.4 Incorporation of passwords and security keys into software

To allow passwords to be changed when needed, passwords must never be hard-coded (incorporated) into software developed by or modified by Alliance University Group workers. Also, the security keys if needed to be added into the software, should be done using some key management system.

2.4.5 Prevention of password retrieval

Computer and communication systems must be designed, tested, and controlled so as to prevent both the unauthorized retrieval and use of stored passwords, whether the passwords appear in encrypted or unencrypted form.

2.4.6 Reliance on operating system user authentication process

Alliance University application systems developers must consistently rely on the password access controls provided by an operating system or an access control package that enhances the security of the application by managing the authentication and authorization process securely. Developers must not construct separate mechanisms to collect passwords and/or user-IDs.

Similarly, developers must not construct or install other mechanisms to identify or authenticate the identity of users without the advance permission of the ITS department.

Developers are prohibited from building or deploying secret user-IDs or passwords which have special privileges and which are not clearly covered in the system documentation.

2.4.7 System access control with individualized passwords

Computer and communication system access control must be achieved via passwords which are unique to each individual user. Access control to files, databases, computers, and other system resources via shared passwords is prohibited.

2.4.8 Changing vendor default passwords

All vendor-supplied default passwords must be changed before any computer, printer, router, switches, wifi's or any other IT system/software/solution being used for Alliance University business.

2.5 Password related user responsibilities

2.5.1 Requirement for different passwords on different systems

To prevent the compromise of multiple systems, computer users must employ different passwords on each of the systems to which they have been granted access.

2.5.2 Don't use same password on different systems

Users must refrain from using the same password on multiple computer systems.

2.5.3 Suspected disclosure forces password changes

Each user must immediately change his or her password if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party. It should also be reported to the ITS department immediately.

2.5.4 Password changes after compromise of a multi-user computer system

If a multi-user computer system employs fixed passwords as its primary access control mechanism, all passwords on that system must be changed immediately after evidence of system compromise has been discovered. At this time, all users must be instructed to change their fixed passwords on other machines, if the passwords on the compromised machine are also used on these other machines. Such compromise should also be reported immediately to the information security office of Thompson Digital.

2.5.5 Writing passwords down and leaving where others could discover

Passwords must not be written down and left in a place where any unauthorized persons might discover them.

2.5.6 Passwords management

All passwords should be stored, accessed and managed through a password management system. Password should not be maintained in a clear text either on software or physical paper or computer file system.

2.5.7 No fixed passwords stored in dial-up programs or internet browsers

Users must not store fixed passwords in dial-up communications programs or Internet browsers at any time.

2.5.8 Password sharing prohibition

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use electronic mail, company cloud storage or local area network servers, and other mechanisms as approved by the ITS Department.

2.5.9 Users responsible for all activities involving personal user-IDs

Users are responsible for all activity performed with their assigned user-IDs. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their user-IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users.

2.6 Password related administrator responsibilities

2.6.1 Forced change of all passwords after system compromise

Whenever a system has been compromised, system owners / custodians / managers must immediately change every password on the involved system. Even suspicion of a compromise requires that all passwords be changed immediately. Under either of these circumstances, a trusted version of the operating system and all security-related software must also be reloaded. Similarly, under either of these circumstances, all recent changes to user and system privileges must be reviewed for unauthorized modifications.

2.6.2 Forced change of all passwords after supervisor account compromise

If a privileged (supervisor) account has been compromised by an intruder or another type of unauthorized user, all passwords on that system must be immediately changed and information security office must be informed.

2.6.3 In-person proof of identity to obtain a password

Passwords must never be disclosed via voice telephone lines. To obtain a new or changed password, a user must show up in person or fill a bona-fide password reset request form and present suitable identification or show up to a local IT person with the ability to request for a new password. One time use password can be emailed to the immediate supervisor after receiving a bona-fide password change request from the user. The supervisor must handover the password in person to the affected employee who has requested for resetting of his/her password.

2.6.4 When and how passwords may be disclosed by security administrators

Security administrators must only disclose passwords if a new user-ID is being assigned, if the involved user has forgotten or misplaced a password, or if the involved user is otherwise locked out of his or her user-ID. Security administrators must not reveal a password unless the involved user has first provided two pieces of definitive evidence substantiating his or her identity along with a bona-fide password reset request form.

2.7 Log-in process

2.7.1 Positive identification required for system usage

All users must be positively identified prior to being able to use any multi-user computer or communications system resources.

2.7.2 Access controls for remote systems connecting to production systems

All computers which have remote real-time dialogs with Alliance University Group production systems must run an access control package approved by the ITS Department.

2.7.3 User-ID & password required for computer-connected network access

All users must have their identity verified with a user-ID and a secret password--or by other means which provide equal or greater security--prior to being permitted to use Alliance University computers connected to a network.

2.7.4 Unique user-ID and password required

Every user must have a single unique user-ID and a personal secret password. This user-ID and password will be required for access to Alliance University multi-user computers and computer networks.

2.7.5 Security notice in system log-in banner

Every log-in screen for multi-user computers must include a special notice. This notice must state: (1) the system may only be accessed by authorized users, (2) users who log-in represent that they are authorized to do so, (3) unauthorized system usage or abuse may subject to criminal prosecution, and (4) system usage will be monitored and logged.

2.7.6 Network log-in banner wording required

The following warning banner must be used when users connect to Alliance University internal computer networks: "This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by systems personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials."

2.7.7 Notice of last log-in time and date

At log-in time, every user must be given information reflecting the last log-in's time and date. This will allow unauthorized system usage to be easily detected.

2.7.8 Prohibition of multiple simultaneous on-line sessions

Unless special permission has been granted by the system manager, computer systems must not allow any user to conduct multiple simultaneous on-line sessions.

2.7.9 Automatic log-off process

If there has been no activity on a computer terminal, workstation, or microcomputer (PC) for twenty (20) minutes, the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided the proper password.

2.7.10Leaving sensitive systems without logging-off

If the computer system to which they are connected or which they are currently using contains sensitive information, users must not leave their microcomputer (PC), workstation, or terminal unattended without first logging-out or invoking a password-protected screen saver.

3 Privilege control

3.1 Use of systems

3.1.1 Granting user-IDs to outsiders

Individuals who are not employees, contractors, or consultants must not be granted a user-ID or otherwise be given privileges to use Alliance University computers or communications systems unless the written approval of a department head has first been obtained.

3.1.2 Third party access to Alliance University systems requires signed contract

Before any third party is given access to Alliance University systems, a contract defining the terms and conditions of such access must have been signed by a responsible manager at the third party organization. These terms and conditions must also be approved by both the local IT Manager and the Local Law Department manager.

3.1.3 When established, outsider user-IDs must have defined expiration date

Every user-ID established for a non-employee must have a specified expiration date. If the systems administrator setting-up such a user-ID is not provided with an expiration date, then thirty days will be used as a default.

3.1.4 Information systems access privileges terminate when workers leave

All Alliance University information systems privileges must be promptly terminated at the time that a worker ceases to provide services to Alliance University from all IT system assets.

3.1.5 Time limits for user-IDs and file retention period after expiration

All user-IDs for multi-user systems at Alliance University to be monitored for retention. HR department to intimate the IT Department for the disabling of the ID's during the off-boarding process. This intimation to include the instructions regarding the date on which the ID is to be disabled and the duration for which relevant data needs to be maintained / archived. Subsequent to the period communicated, the data will be archived / deleted by the IT Department.

3.1.6 Disclaimer of responsibility for damage to data and programs

Alliance Univesity uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems. In keeping with these objectives, management maintains the authority to: (1) restrict or revoke any user's privileges, (2) inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives, and (3) take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the involved users. Alliance University disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

3.2 Information driven access control

3.2.1 Where to use computer system access controls

All computer-resident information which is sensitive, critical, or valuable must have system access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

3.2.2 Personal digital assistant use for corporate business information

Personal Digital Assistants (PDAs), handheld computers, and smart phones must not be used for Alliance University business information unless they have first been configured with the necessary controls and approved for such use by the IT Department. Exceptions will be made for Official E Mails, calendars, address books, and stored connection information such as telephone numbers.

3.2.3 No sensitive information on personal digital assistants, handhelds, etc.

The security mechanisms available on Personal Digital Assistants (PDAs), handheld computers, smart phones, and similar small portable computers have not yet been shown to be effective and reliable. Accordingly, workers must refrain from using these computers with sensitive Alliance University information.

3.2.4 All software must be regulated by access control systems software

All software installed on Alliance University multi-user systems must be regulated by approved access control systems software. This means that a user's session must initially be controlled by approved access control systems software, and if defined permissions then allow it, control will then be passed to separate application software.

3.2.5 Systems requiring password-based access control package

If a small system (PC, LAN, etc.) handles either critical or confidential information, the system must also utilize a properly maintained version of an approved password-based access control system.

3.2.6 Privilege restriction based on the need-to-know

The computer and communications system privileges of all users, systems, and programs must be restricted based on the need-to-know.

3.2.7 Privilege restriction based on the need-to-withhold

Access to Alliance University computer and communications systems will be granted by default to all employees unless the manager controlling a specific system has specifically defined access control rules.

3.2.8 Specific information access policies must be prepared

Designated information owners must establish specific written policies regarding the categories of people who will be granted permission to access information for which they are responsible. These policies must also specify limitations on the use of this information by those to whom access has been granted.

3.2.9 Generic or default administrator user-ids based on job function prohibited

Generic user-IDs based on job function are prohibited. Instead, user-IDs must uniquely identify specific individuals.

3.2.10 Re-use of unique user-IDs prohibited

Each Alliance University computer and communication system user-ID must be unique and forever connected solely with the user to whom it was assigned. After a worker or customer terminates their relationship with Alliance University, there must not be any re-use of the involved user-ID.

3.2.11Limited number of privileged user-IDs

The number of privileged user-IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes. All such accesses to be formally approved by the ITS department of Alliance University.

3.2.12Two user-IDs required for all systems administrators

Multi-user systems administrators must have at least two user-IDs. One of these user-IDs must provide privileged access and be logged; the other must be a normal user-ID for the day-to-day work of an ordinary user.

3.2.13Logging and reporting on privileged user-ID activity

All user-ID creation, deletion, and privilege change activity performed by systems administrators and others with privileged user-IDs must be securely logged and reflected in periodic management reports.

3.2.14 Use of default administrator user-IDs prohibited

Multi-user systems administrators must have personal user-IDs with administrator right. One of these user-IDs must provide privileged access and be logged.

3.2.15 Default administrator user-IDs backup

Multi-user systems administrator's credentials must be stored in secure area (Safety box), used only during emergency case. A procedure of crisis must be implemented including the process to access to the Multi-user systems administrator's credentials. This procedure must be known by the management of Alliance University.

3.3 Other privilege restrictions

3.3.1 Dormant user-IDs and automatic privilege revocations

All user-IDs must automatically have the associated privileges disabled or revoked after a ninety (90) day period of inactivity.

3.3.2 End-user access to operating system commands

After logging-in, all end-users of multi-user systems must be kept in menus which show the options that they have been authorized to select. End-users must not be allowed to invoke operating system level commands.

3.3.3 Contractor or user with temporary contract

Responsibilities should be in place to ensure an employee's, contractor's or third party's users' exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed.
For the temporary contracts, an expiration date must be indicated, and the account must be disabled.

3.4 Synthesis

Properties	Status	Comments
USER Account		
Password	Mandatory	
Multi-Factor authentication	Recommended	
Change password periodically	90 Days	
Password Length[2]	8 Characters minimum and 64 characters maximum. 14 characters for administrative accounts.	
Unique password	Mandatory (3 Versions minimum)	
Simultaneous access	1	
Expiration Date of Account		Mandatory for contractors and 3rd party
User account blocked if "n" fruitless attempts of connection	3	
Grace login	2	
Default password	Mandatory	Must be unique / User
Password change mandatory at the first connection	YES	
SYSTEM &		
Mac address Restriction	Mandatory	If no password for system account
Encrypted password during the communication	Mandatory	Example : Encrypt the http password during the connection
Encrypted password if stored in a file or an application.	Mandatory	
ADMINISTRATOR ACCOUNT		
Password	Mandatory	
Change password periodically	60 days	
Password Length	10 Characters mini	
Unique password	Mandatory (13 Versions mini)	

Grace login	0	
Mac address Restriction	Mandatory	
Secondary responsibility for Passwords of all Administrator Accounts	Mandatory	To be shared with the CIO in a sealed envelope along with a signoff at the time of submission.

4 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5 Review process

This document must be be reviewed yearly.
The review must be performed by the owner of the document.
The final document must be reviewed by the VP and approved by the CIO.

6 Communication process

This document can only be communicated when approved by the CIO

6.1 Glossary

6.2 Advice

This document is a general policy and covers information security concepts at a high level, defines these concepts, describes why they are important. The technical documents describe how to implement this policy locally. If necessary, you must write a procedural document for applying this policy.

ALLIANCE UNIVERSITY

Private University established in Karnataka State by Act No. 34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi

DEPT. OF INFORMATION TECHNOLOGY SERVICES (ITS)

Security Incident Management Policy

10/10/2022

Document Title
Security Incident Management Policy Document Number: IT-POL-SIM-01 Revision Number: V1.0

Prepared by	Reviewed by	Approved by
Shivakumar Totad Asst. Manager -ITS	Yathish Babu K Manager-IT	Santosh T Kawari CIO

Security Incident Management Policy

Reviews follow-up			
Version	**Date**	**Who**	**Item**
Ver 1.0	10-10-2022	Yathish Babu K	Security Incident Management Policy

Related Documents			
Document	**Version**	**Writer**	**Description**

Published / Communicated / Posted			
Document	**When**	**Who**	**Audience**
Security Incident Management Policy	10-10-2022	Santosh T Kawari CIO	

Contents

1 Overview

The purpose of this policy is to develop and implement the Information Security Incident Management process for networks, hardware, cloud, and software, improving user security awareness, early detection and mitigation of security incidents and suggesting the actions that can be taken to reduce the risk due to security incidents.

1.1 Scope

This policy covers the types of incidents described in the table below and applies to all information assets owned by Thomson Digital:

Incident Category	Description
Malware and Social Engineering	• Infection of systems with malware (virus, worm, Trojans) • Spam originating from Alliance University information assets. • Phishing or Smishing attempting to steal personal information.
Security Weakness	• Vulnerabilities that may be exploited by a malicious user or an unauthorized user to gain access caused by: ➢ Misconfiguration of applications, systems, servers or network devices. ➢ Discovery of a new vulnerability that has not been patched. ➢ Non-compliance with a security standard, policy or procedure(s). ➢ Breaches of Physical Security.
System Unavailability/ Disaster	• Any event or activity resulting in or may result in loss of capability of Alliance University to conduct normal business operations, for a period of time extending beyond established service threshold levels due to: o Human errors. o Malfunction of Network, Software or Hardware. o Uncontrolled Changes to the systems, software, applications, servers or network devices.

1.2 Audiences:

IT Team, Assessment Team, Alliance University employees, Vendors and contractors

1.3 Responsibilities and actors

a) Head-ITS of Alliance University shall be responsible for the development and implementation of the controls defined in this policy. Head - ITS shall be SPOC for any IT Security events or Security weaknesses.

b) It is the responsibility of all employees and third parties.

c) staff to report any IT security event or security weakness that they observe or suspect to the Head – ITS.

d) It is the responsibility of Head – ITS to send a security event or security weakness report to the authorized team.

2 Policy

2.1 Objectives

All security breaches or attempts to breach and all discovered security weaknesses in information systems and processing facilities must be reported and recorded. The Information Security Incident Management procedure must ensure that all reported security breaches or weaknesses are responded to promptly and actions taken to prevent recurrence.

The objectives of this policy are to:

a) Develop the proactive measures to minimize the impact of any Incident on information systems and processing facilities;

b) Create the awareness and encourage the users to report the security weaknesses and/or incident that they identify;

c) Enable the proactive management of problems by capturing data that can be used to analyze trends and problem areas, thereby preventing the security incidents to occur; and

d) Learning from the incidents and continually improving the Information Security Incident Management process within Thomson Digital.

2.2 Incident identification

A security incident could be defined as the act of violating the security policy. The following is an illustrative list of what actions can be classified as incidents:

a) Attempts to gain unauthorized access to a system or its data; masquerading, spoofing as authorized users;

b) Unwanted disruption or denial of service;

c) Unauthorized use of a system for the processing, transmitting or storing data by authorized/unauthorized users;

d) Changes to system hardware, firmware or software characteristics and data without the knowledge of application owner;

e) Existence of unknown user accounts. and/ or

f) Unauthorized disclosure of company information

Incident related to physical issues:

a) Breach of preventive physical restrictions, put in place, to minimize the occurrence of information security incidents.

2.3 *Reporting information security event and weakness*

b) All identified information security incidents must be recorded.

a) All employees and third party service staff shall be responsible for reporting the security incidents that they observe or suspect.

b) Employees shall immediately inform to the Head – ITS via email, phone or physically about any incident.

c) Business SPOC shall inform immediately to respective client, if any client data or service got impacted.

2.4 *Assessment and decision on information security events*

a) All reported incidents shall be assessed by the Head – ITS and decided whether to classify the event as a security incident.

b) If it is classified as a security incident, its impact, corrective action, time plans shall be determined.

c) If it is classified as security incident, then all the recorded information should be transferred to the authorized team who is authorized to deal with this incident.

2.5 *Impact and urgency*

The Information Systems at Alliance University are classified in three broad categories. An incident which is similar in nature may have a different impact and recovery urgency, based on the category of the Information system/process. The three broad categories are described below:

2.5.1 *Core assets*

Core assets are assets as required by Alliance University to perform its business process. These core assets include:

a) Applications used by Finance and IT. Application related servers, OS, databases, storage, network and cloud infrastructure.

b) Emails

c) Network services within Alliance University

d) Internet Connectivity

e) Laptops, desktops and other assets used by Alliance University employees in Finance, IT and client service delivery

2.5.2 Business Operation Assets

Business Operations assets are assets which shall be available at most times for enabling business operations. These business assets assist in directly or indirectly performing client service delivery. They include:

a) Physical premises for performing operations

b) Laptops, desktops, dialer servers and other assets used by Alliance University employees for supporting client delivery, and may not have direct impact.

2.5.3 Business Support Assets

Business support assets are assets which contribute to efficient business operations and regulatory compliances; however, they are not required to be available continuously. They include:

a) Laptops, desktops and other assets used by Alliance University employees in HR, Admin and Facilities department

b) Paper documents

c) Tools used for monitoring performance, internal audits etc.

The scheme in the table shall be used for determining the incident's, Impact and Urgency classification as high, medium or low.

Impact	Parameters
High	a) Any Core Business Assets impacted which causes unavailability of more than 4 hours b) Regulatory or legal non-compliance. c) Business operations assets not available for more than 1 day
Medium	a) Any Core Business Assets impacted which causes unavailability of less than 60 minutes b) Business operations assets not available for less than 1 day
Low	a) Core business assets available but not performing as effectively b) Any partial business operational services not available and alternative arrangement exists.

Urgency	Parameters
High	a) Core business assets impacted b) Serious Compliance or security breach as time progresses.
Medium	a) Time barred resolution required b) Risk to core business services critical timelines
Low	a) No Risk to core business services b) No Risk to daily business operations c) No Potential risk to Compliance or policies

The scheme in the table shall be used for determining the incident's, Impact and Urgency classification as high, medium or low.

2.6 Prioritization

Prioritization occurs as a result of assigning a level of Impact and Urgency to the event. In the event of a service disruption, an incident is prioritized by assessing the disruption's impact on the organization and urgency for resolution.

		Impact		
		High	Medium	Low
Urgency	High	Critical	Critical	High
	Medium	Critical	Medium	Medium
	Low	High	Medium	Low

Incident categories:

a) P1 Incidents (Urgency * Impact) = Critical

b) P2 Incidents = High

c) P3 Incidents = Medium, Low

2.7 Response to information security incidents

a) Information security incidents shall be responded by information security office and shall have defined target date of closure date.

b) P1 Incident shall be closed within 24 hours of raising of incidence

c) P2 Incident shall be closed within 72 hours of raising of incidence

d) While P3 shall be closed within 168 hours

e) If there is dependency to third party, the Incidence response time is as per contract agreement.

The detailed process flows for P1, P2 and P3 category of incidents should be covered in the security incident response procedure document.

2.8 Learning from information security incidents

a) The Head – ITS shall establish a knowledge base for the information gained from the evaluation of all information security incidents.

b) The knowledge base shall be referred to for incident handling and as a learning source of information security incidents.

2.9 Collection of evidence

a) As per the legal requirements the evidences shall be collected during the incident analysis, maintained and presented to the relevant authorities of outsourcing team/organization.

b) The evidence shall be collected in a manner that it is complete in all respects, does not destroy its evidentiary value, and can serve as evidence in the court of law.

3 Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment.

4 Review process

This document has to be reviewed yearly.
The review has to be performed by the owner of the document
The final document must be reviewed by the Head-ITS and approved by the CIO.

5 Communication process

This document can only be communicated when approved by the CIO of Alliance University.

5.1 Glossary

SPOC	Single point of contact
ISMS	Information Security Management System
IS	Information Security
ISO	Information Security Office

5.2 Advice

This document is a general policy and covers information security concepts at high level, defines these concepts, describes why they are important. The technical documents describe how to implement this policy locally. If necessary, you have to write procedural document for applying this policy.

ALLIANCE UNIVERSITY

Private University established in Karnataka State by Act No 34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi

DEPT. OF INFORMATION TECHNOLOGY SERVICES (ITS)

E-Mail Policy

10/10/2022

Document Title
Email Policy Document No. IT-POL-EML-001 Revision Number: V1.0

Prepared by	Reviewed by	Approved by
Totad	Yathish	Kawari
Shivakumar Totad Asst. Manager -ITS	Yathish Babu K Manager-IT	Santosh T Kawari CIO

E-Mail Policy

Reviews follow-up			
Version	**Date**	**Who**	**Item**
Ver 1.0	10-10-2022	Yathish Babu K	E-Mail Policy

Related Documents			
Document	**Version**	**Writer**	**Description**

Published / Communicated / Posted			
Document	**When**	**Who**	**Audience**
E-Mail Policy	10-10-2022	Santosh T Kawari CIO	

Table of Contents

Email Policy

1 Introduction

The Alliance University email system is a vital tool for communication and collaboration among students, faculty, and staff. It is also the official channel for receiving important information and notifications from the university administration. Therefore, it is essential that all users of the university email system follow the email policy and adhere to the best practices outlined in this document.

2 Email Policy

The email policy applies to all users of the university email system, including students, faculty, staff, and alumni. The policy covers the following aspects:

- Email ID Management
- Access and security
- Privacy and confidentiality
- Content and etiquette
- Storage and retention
- Monitoring and compliance

3 Email ID Management

3.1 Email ID Creation

The university email ID will be created for all the employees on request of HR department.

The university email ID for students will be created on request from the admissions department or respective deans' offices.

The distribution mail group will be created and managed by exchange administrators for bulk mail communications.

The created email ID will be added to the distribution group for their department/School/Category (Faculty/Staff/Students).

3.2 Email ID Modification

Any modification request mail for the email ID will be approved by the authorized personnel and will be processed by the exchange administrator.

The distribution group membership will also be modified on email request approved by the authorized personnel.

The archiving, forwarding and sharing content from SharePoint and OneDrive will be assisted by exchange administrators upon mail request.

3.3 Email ID Disabling/Blocking

The resigned employee email ID will be blocked on mail communication from HR department.

Any temporary access to be restricted for employees or students will be processed through the mail request from authorized personnel.

The suspected account or potentially affected email accounts will be blocked through policies created and managed by the exchange administrator.

4 Access and Security

All users of the university email system are responsible for maintaining the security and integrity of their email accounts. Users should:

- Use strong and unique passwords for their email accounts and change them regularly
- Never share their passwords or login credentials with anyone else
- Never access or use another person's email account without their permission
- Report any suspicious or unauthorized activity on their email accounts to the IT department
- Use the university email system only for authorized purposes and in accordance with the university policies and regulations

5 Privacy and Confidentiality

All users of the university email system should respect the privacy and confidentiality of the email messages they send and receive. Users should:

- Only send email messages to the intended recipients and avoid sending unnecessary or unwanted messages.
- Use the appropriate level of encryption and security for sensitive or confidential information.
- Not forward or disclose any email messages that contain personal or confidential information without the original sender's or the owner's consent.
- Delete or archive any email messages that are no longer needed or relevant.
- Not use the university email system for personal or commercial purposes that are unrelated to the university activities or interests.

6 Content and Etiquette

All users of the university email system should use proper and professional language and tone in their email messages. Users should:

- Write clear and concise subject lines that reflect the main topic or purpose of the email message.
- Use appropriate salutations and signatures for the recipients and the context of the email message.
- Use correct spelling, grammar, and punctuation in their email messages.
- Avoid using all caps, excessive punctuation, or emoticons in their email messages.
- Be polite and respectful in their email messages and avoid using offensive, abusive, or discriminatory language.
- Not send or forward any email messages that contain spam, viruses, malware, or other harmful content.

7 Storage and Retention

All users of the university email system should manage their email storage and retention efficiently and effectively. Users should:

- Regularly check their email inbox and folders and delete or archive any email messages that are no longer needed or relevant.
- Not exceed the email storage limit assigned to their email accounts by the IT department.
- Not use the university email system as a backup or archive for their personal or professional files or documents.
- Follow the university records management policy and procedures for the retention and disposal of email messages considered official records or documents.
- Not delete or alter any email messages that are subject to a legal hold or a litigation request.

8 Monitoring and Compliance

The university reserves the right to monitor and audit the use of the university email system by its users. The university may:

- Access, inspect, or disclose any email messages or attachments stored or transmitted on the university email system.

- Block, filter, or quarantine any email messages or attachments that are deemed to be inappropriate, harmful, or in violation of the email policy.
- Suspend, terminate, or revoke the email access or privileges of any user who fails to comply with the email policy.
- Report any breaches or incidents of the email policy to the relevant authorities or parties.
- Take any disciplinary or legal action against any user who violates the email policy.

9 Conclusion

The email policy for the university is designed to ensure the proper and responsible use of the university email system by its users. The email policy aims to protect the security, privacy, and reputation of the university and its users. All users of the university email system are expected to read, understand, and follow the email policy and the best practices outlined in this document.

ALLIANCE UNIVERSITY

Email Guidelines and Protocol

Policy Document Number: **AU/REG/2018/001/R1**
Effective Date: August 7, 2018
Revision Date: January 23, 2020

In any institution, flow of information is imperative for effectiveness. To ensure total quality, continuous improvement, and effective communication, the following is a set of guidelines to use when communicating via emails within the University, and to outside recipients and/or vendors.

1. **Group emails**:
   a. Group emails include specific announcements, instructional content, research-oriented, information etc. and require implicit or explicit prior approval.
   b. All faculty shall have access to send group emails to their respective sections / classes that they teach and all Heads of Schools / Departments shall have access to send group emails to their respective schools or departments.
   c. It is the responsibility of the sender of a group e-mail to obtain the necessary approval from the HOD listed below.
   d. We must ensure that the information must be complete, accurate and timely and the information available within various functional groups be routed to key decision centers/makers as the case may be.
   e. The following table lists access to sending group emails and details of approvals and recipients on cc.

Academic Departments:

Sender	Needs the approval of	Recipient (on CC) mandatorily marked
Faculty	HOD	HOD, Dean, Registrar, PVC / VC
HOD	The Dean / Associate Dean	Dean, Registrar, PVC / VC
Dean	PVC / VC	Registrar, PVC / VC

Non-Academic Departments:

Sender	Needs the approval of	Recipient (on CC) mandatorily marked
Department HOD	Reporting Authority / Registrar / PVC / VC	HOD, Registrar, PVC / VC

2. **Response time**: All recipients of any given formal email communication are requested to respond at the earliest but no later than three-working days.

   In the event any employee receives an email which is not concerned with his/her nature of work/key responsibilities, the email must be forwarded promptly to office@alliance.edu.in.

3. **Correctness**: All emails are required to be thoroughly proof-read and error-free (in terms of grammar, spellings and information) before sending it to the concerned recipients.

4. **Individual Emails:** Any individual sending an email has to take complete responsibility for the content, accuracy of information and must ensure confidentiality at all times.

   It is expected from every team member at Alliance University that they make use of their judgement to determine who the audience must be and must not be forwarding emails or marking copies to people not concerned with the same.

   a. Individual emails to students, colleagues or external entities include sharing of details, information, creating meetings / calendars, responding to queries, soliciting or sending proposals from partners / vendors, etc. require implicit or explicit approvals.

   b. The sender of an email needs to use his/her judgement to discuss, solicit views or obtain necessary approvals from the HOD as listed below as these might have responses that have obligations attached.

   Academic Departments (Emails that need attention/escalation):

Sender	**Needs the approval of**	**Recipient (on CC) mandatorily marked**
Faculty	HOD	HOD, Registrar, PVC / VC
HOD	The Dean / Associate Dean	The Dean / Associate Dean, Registrar, PVC / VC
Dean	PVC / VC	Registrar, PVC / VC

   Non-Academic Departments (Emails that need attention/escalation):

Sender	**Needs the approval of**	**Recipient (on CC) mandatorily marked**
Staff	HOD	HOD, Registrar, PVC / VC
Department HOD	Reporting Authority / Registrar / PVC / VC	HOD, Registrar, PVC / VC

5. **Sensitive Information**: All faculty and staff are required to treat sensitive and confidential information with utmost discretion and such email communication(s) are not to be shared and/or forwarded to others within or outside the University.

   However, in case of extenuating circumstances, you are requested to consult with the PVC / VC before sharing such information with other parties.

6. **Signature**: All faculty and staff are required to follow a standard signature (as shown below) for all email communication, in order to maintain uniformity and conformity.

These guidelines are to be followed with immediate effect and adherence to the same is appreciated.

ALLIANCE UNIVERSITY

Madhu Sudan Mishra
Registrar
Alliance University
P: +91 80-46199101; 46199100
A: Chandapura - Anekal Main Road, Anekal, Bangalore - 562106
W: www.alliance.edu.in E: registrar@alliance.edu.in

#3	#10	#10	
Best B-School under Private University (Times B-School Survey 2019)	**Best Private University in India (India Today, 2019)**	**Best B-School in India offering Global Business Courses (Outlook Magazine, 2018)**	QS I·GAUGE Teaching & Learning Employability Facilities DIAMOND