10 YEARS OF UNIVERSITY RECOGNITION
20 YEARS OF ACADEMIC EXCELLENCE

REVA UNIVERSITY
Bengaluru, India

IT POLICIES & GUIDELINES

Rukmini Knowledge Park
Kattigenahalli, Yelahanka, Bengaluru - 560 064
www.reva.edi.in

There are four documents each describing certain IT policy. The titles of the document are:

1. Acceptable Use Policy
2. Information Technology (IT) Procurement Policy
3. Standard Nomenclature – Email
4. Log Policy

1.	Officer Responsible with contactdetails	Head, Department of IT
2.	Department responsible with contactdetails	Department of IT AD.DOIT@reva.edu.in
3.	Approved by	Board of Governors during the BoG Meetingheld on 19-06-2020
4.	Signature of the Chancellor (Chairman-Board of Governors)	

ACCEPTABLE USE POLICY

(Including Some Important Guidelines)

INDEX

1	Objective	6
2	Scope	6
3	Policy Provisions	6
3.1	Appropriate Use	6
3.2	Authorized Users	6
3.3	Responsibilities of Authorized Users	7
3.4	Access to IT Facilities	7
3.5	Accessing the Internet and Online Services	7
3.5.1	Internet and Online Services Access Restrictions	7
3.6	Copyright Provisions	8
3.6.1	REVA University IT Services, Facilities, and Infrastructure Provisions in Relation to Copyright Protected Material	8
3.6.2	Responsibilities of REVA University Members in Relation to Copyright Protected Material	9
3.6.3	Dealings in Copyright Protected Material for Teaching or Research	9
3.6.4	Private Use Conditions and the REVA University	9
3.6.5	Notices of Copyright Infringement	9
3.7	Modification of IT Services, Facilities and Infrastructure	10
3.7.1	Unauthorized Modifications of IT Services, Facilities and Infrastructure	10
3.8	Use of BYOD IT Devices	10
3.8.1	Connection to Networks	10
3.8.2	Connection Restrictions	11
3.8.3	Connection Disclaimers	11
3.9	Software Installation on REVA University IT Facilities and Devices	11
3.9.1	Authorized Software	11
3.9.2	Unauthorized Software	12
3.9.3	Unlicensed Software	12
3.10	Monitoring of IT Services, Facilities and Infrastructure	12
3.11	Privacy	12
3.12	Breaches	13
4	Responsibilities	13
	Annexure-1: Acceptable Use Agreement	14
	Annexure-2: 15 Email Etiquette Rules Every Professional Should Follow	16

1. OBJECTIVE

The purpose of this document is to ensure the appropriate use of REVA University's Department of IT Services and define the responsibilities of users of the REVA University's ITServices and Infrastructure.

The objective of this Policy, and associated procedures are to define:

1. Access to, and use of University IT Services
2. The responsibilities of users regarding the appropriate use of IT Services and
3. The responsibilities of users in maintaining the good name of REVA University

2. SCOPE

This policy applies to all the members of faculty, staff, students and associates of REVA University

3. POLICY PROVISIONS

IT Services, Facilities and Infrastructure are provided in support of University activities including research, teaching and learning, and operational activities. The conditions of use defined in this Policy, and associated IT Policies and Procedures, apply to all REVA Universitymembers, all IT Services provided by the University, all Facilities and Infrastructure owned bythe University, and to any BYOD Device that connects to University Infrastructure.

3.1 APPROPRIATE USE

REVA University IT Services must be used in an appropriate manner. Appropriate useis considered to be the use of equipment in:

- A legal manner, meeting the requirements of legislation and University By-laws, Ordinances and Policy and
- Meeting the principles of fair use

3.2 AUTHORIZED USERS

Acceptable are only available for use by Authorized Users. An Authorized User is anindividual that has a legitimate relationship with REVA University as defined in REVA University Statutes. All Authorized Users are bound by the Acceptable Use Policy.The Acceptable Use Policy becomes binding when:

- Faculty members and staff members and associates accept their offer ofemployment or appointment

- Students get enrolled after paying the prescribed University fee

All members must sign the Acceptable Use Agreement and returned to IT Services inorder for any member permission to be granted as Authorized User status.

3.3 RESPONSIBILITIES OF AUTHORIZED USERS

REVA University IT Services must be used in a manner which supports the good nameof the University and may only be used:

- In support of teaching, learning, research, personal or professional development, University operations and management or other activities officially directed towards the mission of the University and
- For limited personal use

All Authorized Users of University IT Services must respect the rights of other Authorized Users to ensure that all have equitable privileges, privacy and protectionfrom interference or harassment.

3.4 ACCESS TO IT FACILITIES

All members of the University can access Acceptable as per the rules of the University. Physical access to IT Facilities is managed through the University's security arrangements. Access to buildings and computing laboratories is at the discretion of the relevant School Director/Administrator.

3.5 ACCESSING THE INTERNET AND ONLINE SERVICES

Access to the Internet, and services provided via the Internet, are available to Authorized Users only. Use of the Internet and associated services are provided under the conditions of appropriate and ethical use. Users of this service must respect the rights of other Authorized Users to ensure that all have equitable privileges, privacy and protection from interference or harassment. Internet usage must be legal and comply with the requirements of all Central and State Government legislation, University Ordinances, Policies, and Procedures.

3.5.1 INTERNET AND ONLINE SERVICES ACCESS RESTRICTIONS

REVA University reserves the right to block access to internet services, or websites,where accessing, or obtaining content from, those services or

websites using REVA University IT Services, Facilities, or Infrastructure would be considered a breach of Central or State legislation, or a breach of REVA University Policy. REVA University reserves the right to block access to any online service which is identified as a platform for the distribution of viruses, malware, other malicious software, or is associated with solicitation of personal or financial information. The University will make attempts to ensure any internet service, or website, which is blocked is not used for research, teaching and learning, or University business reasons. All accessrestrictions will be approved by the Director, IT. Reviews of access restrictions will be heard by the Director, IT.

3.6 COPYRIGHT PROVISIONS

REVA University expressly forbids the use of any of its IT Services, Facilities and Infrastructure for any purpose which would breach copyright in any way.

The University considers copyrighted materials to include, but not be limited to:

- Music
- Movies
- Television programs
- Electronic publications of E-books
- Electronic journal papers
- Computer software
- Unlicensed data, including unlicensed research data.

.

3.6.1 REVA UNIVERSITY IT SERVICES, FACILITIES, AND INFRASTRUCTUREPROVISIONS IN RELATION TO COPYRIGHT PROTECTED MATERIAL

REVA University IT Services, Facilities, and Infrastructure may not be used todownload, copy, compress, store, transfer or redistribute content without the express permission of the copyright owner. The University reserves the right to remove any alleged infringing material from any of its IT Services, Facilities, and Infrastructure without prior notification. Where a service or website, external to the University, is identified as a source of infringing material the University reservesthe right to block access to that service or website.

3.6.2 RESPONSIBILITIES OF REVA UNIVERSITY MEMBERS IN RELATION TOCOPYRIGHT PROTECTED MATERIAL

Members of the University are prohibited from using any University IT Services, Facilities or Infrastructure to acquire, store or share materials that infringe the rights of the copyright holder. Members may, on occasion, purchase materials via online distributors using University IT Services, Facilities and Infrastructure. These materials may be stored on University Facilities in accordance with the license conditions under which they were purchased. It is the responsibility of REVA University Members to ensure they manage their copyrighted materials in accordance with legislative and policy requirements.

3.6.3 DEALINGS IN COPYRIGHT PROTECTED MATERIAL FOR TEACHING ORRESEARCH

REVA University holds licenses which allow certain copyrighted material, including text, images, music and recorded broadcasts, to be copied, stored and communicated for the educational purposes of the University. Staff and students are obliged to abide by the license conditions for the use of this material. Information regarding the use of copyrighted material for educational purposes may be sought from REVA University Library.

3.6.4 PRIVATE USE CONDITIONS FOR REVA UNIVERSITY

University owned IT Services, Facilities and Infrastructure are owned by the REVA University, not by individuals. Therefore, regardless of whether an individual ownsan original copy of a recording, digital copies may not be stored on any REVA University IT services, Facilities or Infrastructure items. Members of the University may use University IT Facilities and Infrastructure for private listening purposes, butmay not store, or distribute materials. Private media libraries must be held on devices owned by the Member.

3.6.5 NOTICES OF COPYRIGHT INFRINGEMENT

REVA University makes all attempts to ensure copyrighted materials are used within license conditions, and that Acceptable are not used to facilitate copyright breach. All materials, including non-infringing materials and IT equipment is subject to removal from REVA University network in the event that a notice of copyright infringement is delivered against the University. Should the University receive a notice of copyright infringement the University reserves the right to remove the material in question, or make it unavailable by disconnecting the underlying IT Infrastructure via logical or

physical action, until such time that a determination about the legitimacy of the infringement claim can be made.

3.7 MODIFICATION OF IT SERVICES, FACILITIES AND INFRASTRUCTURE

Network modifications shall only be made following written approval by the Head ofIT. Network modifications may only be carried out by an IT Engineer/ Helpdesk Analyst.

3.7.1 UNAUTHORIZED MODIFICATIONS OF IT SERVICES, FACILITIES ANDINFRASTRUCTURE

All network modifications performed without authorization from a Senior Officer or by an unauthorized person are prohibited. Unless part of an approved network modification under section 3.7 above, the installation of a port splitter or any network communication device that supports multiple simultaneous connections to a single network port or third-party network(s) is expressly prohibited. Examples of modifications include, but are not limited to:

- Disconnecting computers from the University network
- Connecting unregistered devices
- Connecting hubs, switches or port splitters

Where an unauthorized modification is detected, a breach of policy may be pursuedand connectivity to a network port may be terminated.

3.8 USE OF BYOD IT DEVICES

REVA University allows Authorized Users to connect privately owned Devices to REVA University IT Infrastructure as per BYOD Policy. The devices need to be configured and tested by Department of IT before connecting to the REVA network/domain. User needs to follow the policy, procedures and practices definedin BYOD Policy.

3.8.1 CONNECTION TO REVA UNIVERSITY NETWORK

In cases where a BYOD Device is to be connected to REVA University network the following conditions apply:

- Device needs to be tested and verified by IT team for the Software Installed.
- All software needs to be Licensed, no unauthorized application.
- User need to get all application and agents required for security and

Compliance purposes.

- Antivirus client needs to be installed in user machine from University CentralConsole.
- Users must adhere to REVA University Policies and Procedures while connected to REVA University network.

Maintenance of Private-owned machines will be user own responsibility, REVAUniversity and IT Team can't be held responsible for the management and maintenance of BYOD Devices connected to REVA network.

3.8.2 CONNECTION RESTRICTIONS

No BYOD Device will access to student databases, staff databases or financial systems, except systems provided with a self- service interface for the User. BYOD Devices may only have access to IT Services or data stores where the Data Custodianauthorizes such a connection to occur, or the IT Service or data store provides a self-service interface for the User.

3.8.3 CONNECTION DISCLAIMERS

REVA University shall not be held responsible for damage or loss to BYOD Devices. IT Team/ Help desk Analyst have the right to disconnect BYOD Devices from REVA University networks and network in the event of a breach of REVA University IT Policy or any other Ordinance, Policy or Procedure of REVA University. The IT Security Manager has the right to request disconnection of any BYOD Device connected to any network of REVA University.

3.9 SOFTWARE INSTALLATION ON REVA UNIVERSITY IT FACILITIES ANDDEVICES

REVA University IT Facilities and Devices operate with a standard, or known, operating environment. This environment is created and configured to allow a Device to support Authorized Users in their work, and to integrate with REVA University IT Services. Any changes to this environment, such as additional software or configuration changes, must be authorized, and preferably actioned, by an IT Team/ Help desk Analyst.

3.9.1 AUTHORIZED SOFTWARE

Authorized software is considered to be software that meets the following conditions:

- The software is used in accordance with license terms & conditions.
- The software has been tested by an authorized IT Team/ Help desk Analystto ensure functionality and security of IT Facilities
- The software has been installed by an authorized IT Team/ Help desk Analyst
- The installation of the software has been authorized by an IT Team/ Helpdesk Analyst

3.9.2 UNAUTHORIZED SOFTWARE

Unauthorized software is considered to be any software that:

- Used in breach of software license agreements
- Not been tested by an authorized IT Team/ Help desk Analyst
- Not installed by an IT Team/ Help desk Analyst or
- Not been authorized by an IT Team/ Help desk Analyst

3.9.3 UNLICENSED SOFTWARE

Unlicensed software is considered to be all software used outside of the license agreement that accompanies the software. The use of unlicensed software on REVA University IT Facilities is strictly prohibited, and any instance immediately renders the software unauthorized. The installation and use of unlicensed softwarecannot be authorized by any person. The software may not be installed or used untilthe conditions of the license have been met. Any software installed or used in violation of license terms shall be deemed unauthorized software and will be in breach of this policy.

3.10 MONITORING OF IT SERVICES, FACILITIES AND INFRASTRUCTURE

All usage of IT Services, Facilities and Infrastructure will be monitored. Information related to the usage of IT Services, Facilities and Infrastructure will be stored and may be used to ensure or investigate compliance with University Policies, Proceduresand Guidelines and relevant State and Central legislation, REVA University may collect information related to the use of IT Services, Facilities and Infrastructure.

3.11 PRIVACY

Information related to REVA University Acceptable is collected and may be consulted to ensure compliance with University policies, procedures and guidelines, and relevant State and Central legislation. This information may be

accessed for purposes of investigating allegations of misuse. Information may be provided to law enforcement agencies where necessary to investigate or report suspected unlawful activity, as per REVA University Policy.

3.12 BREACHES

Breach of this Policy may result in disciplinary action, as provided for under the applicable Employment Agreements and Ordinances. Staff, students and associates learning of any violation of this Policy are obligated to bring this matter to the attention of an appropriate staff member within the University without delay.

4. RESPONSIBILITIES

Head of IT Department is responsible for:

4. Implementation
5. Compliance
6. Monitoring and evaluation
7. Development and/or review
8. Interpretation and advice.

ANNEXURE-1

ACCEPTABLE USE AGREEMENT

Scope and Purpose of this Agreement

Users of Acceptable p rovided by REVA University must be aware of the conditions underwhich access is provided. These are detailed in REVA University Acceptable Use Policy

Acceptable

REVA University Acceptable are covered by this agreement. These include:

- **Services**: All systems supporting interaction, information provision, information storage, or communications provision and the IT Facilities on which they operate.
- **Facilities**: All computers, terminals, telephones, end host devices, licenses, centrally managed data, computing laboratories, video conference rooms, and software owned or leased by the University.
- **Infrastructure**: All electronic communication devices, networks, data storage, hardware, and network connections to external resources such as Internet.

Conditions of Access

All authorized users must comply with the conditions for use of Acceptable as set out in REVA University IT Policies and Procedures including:

- Appropriate use;
- Use only for REVA University related activities and limited personal use;
- Respect for the rights and privacy of other users; and
- Compliance with all relevant State and Central laws and REVA University Ordinances and Policies.

Signature of User

By signing below, I acknowledge that I have read and understand REVA University Acceptable Use Policy. I understand and acknowledge that should I not fulfil all my obligations I will be in breach of this Agreement, which may result in the termination of this Agreement and withdrawal of IT access privileges.

Name: ……

Position or Program with UID Number ……

Signature: …… Date: ……/…… /20….

ANNEXURE-2

15 Email Etiquette to be followed by every professional at REVA

1. Include a clear, direct subject line.
2. Use a professional email address.
3. Think twice before hitting 'reply all.'
4. Include a signature block.
5. Use professional salutations.
6. Use exclamation points sparingly.
7. Be cautious with humor.
8. Know that people from different cultures speak and write differently.
9. Reply to your emails--even if the email wasn't intended for you.
10. Proofread every message.
11. Add the email address last.
12. Double-check that you've selected the correct recipient.
13. Keep your fonts classic.
14. Keep tabs on your tone.
15. Nothing is confidential--so write accordingly.

REVA UNIVERSITY
Bengaluru, India

INFORMATION TECHNOLOGY (IT) PROCUREMENT POLICY

(Including Some Important Guidelines)

INDEX

1	Purpose	19
2	Scope	19
3	Introduction:	19
4	Substantial IT Investment	19
5	Policy / Guidelines	20
6	It Procurement Authorization Form	23

HARDWARE AND SOFTWARE PROCUREMENT POLICY

PURPOSE

The purpose of this policy is to ensure the safety and reliability of university systems and data.This document defines the process through which institutional hardware and software purchases are made.

SCOPE

This policy applies to any purchases of hardware or software using university funds.

INTRODUCTION

The Trust has agreed standards in place for desktop software, operating systems, computer networks and computer hardware and peripherals, such as printers.

This standardisation is essential as it allows the Trust's IT Department to provide a quality service. The main benefit areas are:

1. IT Support Staff are familiar with hardware and peripherals, thus understandingthe requirements and speeding up the procurement process
2. The IT Department is able to stock standard spares in order to reduce down time
3. Network installations are planned and coordinated centrally by experiencednetwork engineers
4. IT staff with relevant skills are recruited.

This policy outlines the procedures that must be in place to achieve these benefits and to ensure the purchase, delivery and installation of IT equipment is coordinated successfully. This policy has been developed in conjunction with the Purchase Department.

SUBSTANTIAL IT INVESTMENT

Where projects for IT, or IT related, equipment (hardware, software or updates to existing hardware or software) are undertaken within the Trust; these projects MUST BE managed using the Project Management methodology and a member of the IT department will need to be included on the Project Board.

POLICY / GUIDELINES

The standard operating procedure covers the following

5. The User / User department will raise an indent in the ERP/PIMS application for purchase of any IT related Hardware / Software with justification to meet the business requirement / continuity.
6. The indent duly approved by the user manger is sent to IT department for processing
7. IT department will check the available stock and if available in stock whether it meets the user requirements.
8. IT department will get quotation from atleast 3 vendors for comparison and evaluate the same, to check whether it meets the user requirements
9. IT department will check the specifications and the price without compromising on quality, delivery and service.
10. IT team will assess the ROI in consultation with the user department
11. Once the negotiation with the vendors are complete and zeroing in on one of thevendors, IT department will issue the purchase order.
12. IT department will ask the vendor to take into consideration the delivery schedulebased in force majeure, like Covid19 like situations, flood, riots etc.
13. The proforma invoice is sent for approval from the management
14. IT department is responsible for taking the delivery of the equipment / software / IT peripherals. Any damage to the goods shall be returned back and replacementis sought from the vendor.

Roles and Responsibilities

15. Software purchases require IT involvement if any of the following are true:

    a. Assistance will be required to install or implement the software.
    b. Software or data used by the software will be stored on an internalserver.
    c. Software will use and/or store data other than “Directory Information”as defined here.
    d. Software or hardware will require campus credentials (Active Directoryor Single Sign On) for authentication.
    e. Software or hardware will be made generally available to studentsand/or employees.
    f. Integration with other campus systems is required.
    g. Ongoing support from IT is expected

16. IT department will be owner of all IT related equipment / peripherals / software etc., in the campus and is responsible for issuance, maintenance, tracking of all IT related goods as per Management Guidelines and approvals.
17. IT department will ensure Minimum Order Quantity of some of the critical items required for business continuity and will re-order when it reach the MOQ
18. IT department will maintain an asset register for IT related equipment / goods
19. IT department will maintain the ageing of the goods required for replacement
20. IT department will coordinate installation at REVA University network.
21. As needed, IT will draft a scope of work that outlines:

    a. Requirements for implementation of the hardware or software.
    b. Expected milestones and timelines.
    c. Levels and expectations for post implementation support.

IT generally does not support hardware and software that have been purchased without ITinvolvement. Support for such systems would be best effort and only as time allows.

Accessibility

1. Software and non-peripheral hardware purchased by the university shouldconsider accessibility as a factor in purchasing decisions.
2. Hardware or software purchased by the university should comply with AICTENorms and Industry best Practices:
3. The office making the purchase will provide to IT:

    a. Documentation regarding accessibility supplied by the vendor.
    b. A list of any exceptions to the above accessibility standards identified inthe vendor documentation.

4. In the event that no suitable product is found that meets minimum accessibility requirements, a description of the reason the product was selected should be submitted to IT. IT will store this documentation for the duration the product is in use.

All purchasers of computer hardware and software It is the responsibility of the users linemanager to ensure that this policy is adhered to, IT hardware or software cannot be donated.

IT Department - It is the responsibility of the Head of IT to ensure that this policy is adheredto, and that IT hardware or software is purchased in accordance with this

policy only.

Supplies Department - It is the responsibility of the Supplies Department to ensure that all purchases of IT equipment and software have been made in accordance with this policy.

Training and Awareness

The requirement of this policy will be brought to the attention of staff via the Trust's inductiontraining program.

This policy will be brought to the attention of all staff responsible for purchasing and procuringIT equipment.

A copy of this policy will be available to all staff via the University's Internet/ Intranet webpages.

Review

This policy will be reviewed in 3 years time. Earlier review may be required in response to exceptional circumstances, organizational change or relevant changes in legislation or guidance.

Monitoring

Monitoring of compliance with this policy will be the responsibility of the Head of IT

Enforcement

The IT Department reserves the right to send back to the supplier, at the budget holders expense, any IT hardware and software purchased outside the guidelines stipulated in this policy where the installation of such equipment/software would be detrimental to the operation of the University IT infrastructure or will impact in the University's effective delivery of business practices.

Discipline

Any breaches of this policy will be brought to the attention of the relevant Head of Department / Management

Breaches of this policy will be investigated and may result in the matter being treated as a disciplinary offence under the University's disciplinary procedure.

IM&T03A

REVA UNIVERSITY

IT PROCURMENT AUTHORISATION FORM

In line with the IT Procurement Policy, no hardware, software or peripherals canbe purchased without the agreement of the IT Manager.

Name of user:	
Department:	
Financial Code:	

Description of hardware, software and/or peripherals required: (please include supplierand part details or attach a copy of the requisition)
Reason the hardware, software and/or peripherals are required:

Name of Manager:_____Signature of Manager: _____

Date required:___/___/____

For IT Department use only: Date request received:__/___/____

Approved:

Declined (Outline reason below) (tick accordingly)Changed to requirements (Outline reason below)

Outline reasons for decline or change to requirements options above:

Proposed installation window: _____

Signature of Head of IT: Date of approval:___/___/____

SJP/SGT

This form will be kept by the IT Department for administrative purposes

REVA UNIVERSITY
Bengaluru, India

STANDARD NOMENCLATURE

Email ID

(Including Some Important Guidelines)

INDEX

1	Introduction	27
2	Policy details	28
3	Generic email addresses and mailboxes	29
4	Additional Information	31
5	Factors considered when creating this naming standard	31
6	Advantages	32
7	Uniqueness & degree of personalization	32
8	Intuitive	33
9	Risk of error	33
10	Administrative costs	33

INTRODUCTION

REVA University has adopted Information transformation journey with implementation of e-learning technology and Industry best practices. As part of the best practices, REVA University has naming standard for REVA email addresses.

Email addresses are made up of two parts separated by "@": local part @ domain.

REVA email addresses have a standard for student addresses: student number @ schoolname.reva.edu.in

Staff addresses also follow, on the other hand, varied widely in format:

- first initial surname @ reva.edu.in
- surname initial @ reva.edu.in
- Department initials @ reva.edu.in
- given name @ reva.edu.in
- surname @ reva.edu.in
- Designation. Department @ reva.edu.in

Accordingly, the staff email address will conform to the approved standard, details of which are given in the sections that follow:

1. NAMING STANDARD

1.1 REVA has implemented the following naming standard for REVA email addresses:

- Undergraduate, Honours, Masters and doctoral students:

  SRNNUMBER@ schoolname.reva.edu.in

- Staff and Post-doctoral fellows:
  - PreferredFirstName: Surname@reva.edu.in,e.g., ram.kumar@ reva.edu.in
  - 1st instance of duplication: Full initials.surname@ reva.edu.in,e.g., ramesh.k@ reva.edu.in
  - 2nd instance of duplication: Full initials.surname2@ reva.edu.in,,e.g., ramesh.k2@ reva.edu.in
  - 3rd instance of duplication: Full initials.surname3@ reva.edu.in,e.g., ramesh.k3@ reva.edu.in

1.2 Domain

Adopting a single domain name "reva.edu.in" for both staff and students offersthe following benefits:

- It promotes a single institutional identity and unity.
- It is far more intuitive and predictable, particularly for people external to REVA, as it requires no knowledge of REVA's organizational structure or IT infrastructure.
- Because it is independent of the organizational structure, it would not need to be changed when departmental names change or when employees change jobs within REVA.
- It reduces administration in a number of ways. Most importantly, having a unique domain name allows for automated email account administration. It would also decrease the work required to maintain backward compatibility for addresses that need to be changed when departmental names change

1.3 Local Part: Students

1.3.1 The student number (CampusID in ERP) continues to be used as the local part of the email address for students. This guarantees uniqueness, clearly differentiates a student email address from a staff address, and allows for automatic mailing from systems that contain the student number such as ERP.

1.4 Local part: students

For staff, the local part takes the form of PreferredFirstName.Surname. Theinformation used to derive email addresses would come from ERP, or the Third Party System.

To ensure that other systems can process our email, we must handle specialcharacters as follows:

1.4.1 Surnames containing multiple words will consist of the full surname with no spaces. e.g: John van der Merwe will be john.vandermerwe@reva.edu.in

1.4.2 Surnames containing special characters not allowed by the email system willbe formatted without the special character. (e.g.: Patrick O' Brian willbecome patrick.obrian@reva.edu.in).

1.4.3 Because email addresses aren't case-sensitive, using "." is also a better option than trying to use caps to differentiate between first and last names(e.g. JoAndersen@reva.edu.in). When typed in lower case only, the name becomes difficult to interpret (e.g. joandersen@reva.edu.in).

2. GENERIC EMAIL ADDRESSES AND MAILBOXES

2.1 Faculties and departments may request generic email addresses. Dedicated mailboxes will be allocated for each faculty Dean, Director and department (HOD).

2.2 Responsibility

2.2.1 The accountability and responsibility for generic addresses resides with the Dean/Director/HOD/Highest authority of the Department responsible for the faculty or department requesting the generic address.

2.2.2 It is the responsibility of the faculty and/or the school/ Department concerned to validate that they are able to adopt the address and that no conflict with any other faculty or department generic email address exists.

2.2.3 Provided that the request has been authorized by a Dean/Director/Supervising Head, and no obvious clash or problem exists, the address and mailbox will be authorized and provided

2.2.4 ICTS will only veto a request if it is technically impossible to implement, and/or encompasses another academic or administrative function or service.

2.3 Format of Generic email Addresses

2.3.1 Vice-Chancellor, Pro-Vice Chancellor and Registrar

- The generic email address for the Vice-Chancellor will bevc@reva.edu.in
- Pro Vice-Chancellors will be granted a generic email address Provc@reva.edu.in.
- Registrar will be granted a generic email address registrar@reva.edu.in.

2.3.2 Academic functions

- **Deans**
    - dean.@reva.edu.in. e.g. dean.iq@reva.edu.in for the Dean of Internal Quality and staff development.
    - Where the title of the faculty is exceptionally long, it may be abbreviated e.g. dean.tpp@ reva.edu.in for the Dean of Training, Placement and Planning and dean.pnd@ reva.edu.in for the Dean of Planning & Development.

- **Graduate School of Business**
    - director.gsb@reva.edu.in for the Director of Graduate School of Business
- **Directors/ Heads of Department**
    - Director/ head.@ reva.edu.in e.g. Director/ head.Archaeology@ reva.edu.in for the head of the department of Archaeology and Director/ head.computerscience@ reva.edu.in for the head of the department of Computer Science.
    - Where the title of the department is exceptionally long, it may be abbreviated e.g. Director/ head.mcb@ reva.edu.in for the head ofdepartment of Molecular and Cell Biology.

2.3.3 PASS departments and university-level functions

For Example:

- registrar@ reva.edu.in for the registrar's office;
- director.finance@ reva.edu.in for the Executive Director Finance;
- director.hr@ reva.edu.in for the Executive Director Human Resources;
- human.resources@ reva.edu.in for the human resources department:

2.3.4 Functional Offices

- @ reva.edu.in e.g. admissions@ reva.edu.in for the admissions office,and fees@ reva.edu.in for the fees office.

2.4 Existing Generic Email Addresses

2.4.1 Where generic email addresses have been implemented as aliases toselected accounts, such addresses will be retained and linked as an alias to a dedicated mailbox associated with a standardized generic email address upon request.

2.4.2 Published generic email addresses which do not conform to the standard must be replaced by an address which conforms to the generic emailaddress standard outlined above.

3 MAINTAINING EXISTING EMAIL ADDRESSES

3.1 Aliases to existing email addresses can be established, so that email messages sent to the old addresses aren't lost. However, this should only be maintained fora limited time. The simplest and most cost-effective solution would be to use the existing email system infrastructure to forward mail to new addresses for a minimum of twelve months.

3.2 After the 12 month period, the email system could generate automated replies topeople who have sent mail to old addresses, to inform them of the new email address naming standard implemented a year previously and to provide a URL forobtaining current REVA email addresses

ADDITIONAL INFORMATION

Factors considered when creating this naming standard

All email address formats have advantages and disadvantages. The table below describesimportant factors to consider in evaluating the various options.

Uniqueness	Each address must be unique; therefore, the naming standard should minimize duplications.
Personalized	Addresses should depersonalize users as little as possible (e.g. anaddress containing only numbers is less personal than one containing a name).
Intuitive	Addresses should be easy to guess and remember, and should notbe too long.

Unchanging	Addresses need not to be changed when the organizational structure changes (e.g. when a department changes names) orwhen a user takes on a new post in the University.
Administrative costs	The management (creation, deletion, editing) of email addresses forboth staff and students should be automated to reduce administrative costs and improve accuracy. It will optimize recurringcost in changing email IDs repeatedly.
Risk of error	Addresses should not cause confusion about the identity of the addressee or make it likely for someone to receive another's email.
Institutional image	Addresses should present a professional image.
Internationally acceptable	Addresses should follow international standards to the extent required to ensure that other email systems can deal with REVA'smail.

ADVANTAGES

Uniqueness & Degree of Personalization

- The standard minimizes the number of duplicate names that would occur, and personalizes addresses as much as possible.
- Using both a given name and a surname generates far fewer duplicates than standards that use less information such as surnames with or without initials, given names only, etc. The ERP data (at the time of implementation) indicated that given name. Surname wouldlead to duplicates, out of 5404. Using a preferred first name instead (e.g. Andy instead of Andrew, Thanda instead of Thandabantu) would reduce some of these duplications, personalize the address and make it more intuitive.
- Using full initials. surname to handle the first duplicate eliminates the number of conflicts to none (again, based on ERP data, which may not be perfectly accurate). This is preferable to attempting to include both a given name and an initial. A format such as naomi.g.jacobs@reva.edu.in that includes two full stops would prevent automation.
- The least personal addresses, which include a number, should occur very rarely.
- To personalize the address, name changes (due to marriage for example), would be allowed.

INTUITIVE

- The given name.surname is widely used internationally.
- Using names rather than numbers, both a first and a last name, and a preferred first namerather than a "given name" makes it much easier for a sender to accurately predict and remember a recipient's email address. Unchanging
- Email addresses would only need to change when an official change of name has taken place (e.g. marriage or divorce). An alias could be created and maintained for six monthsto the old email address. The time period needs to be brief, so that fewer duplicates are created while additional old addresses are being maintained.

RISK OF ERROR

- Errors occur when senders guess addresses incorrectly. By including both a first and lastname, this should happen less frequently than it would if less information was included.
- Errors are most likely to occur in the rare case of an email address containing a number.

ADMINISTRATIVE COSTS

- The naming standard allows for the highest level of automation, thus ensuring consistency, accuracy and lower administrative costs.

REVA UNIVERSITY
Bengaluru, India

LOG POLICY

(Including Some Important Guidelines)

INDEX

1	Overview	36
2	Purpose	36
3	Scope	36
4	General Requirements	36
5	Activities to be logged	38
6	Formatting, Transmission and Storage	39
7	Retention	40
8	Policy Compliance	40

OVERVIEW

Logging from IT systems, applications and services can provide key information and potential indicators of service affecting events, cyber security incidents and compromise.

Although logging information may not be viewed on a daily basis, it is crucial to have appropriate logs retained from a response, investigation and forensics standpoint.

Legislation, formal audits and IT Security team requirements have highlighted the need to produce a formal document relating to effective collection, treatment and retention of thesesystem logs. This policy states the requirements and covers a process for compliance exceptions.

PURPOSE

The purpose of this Policy document is to introduce and enforce procedures to identify specific requirements that information systems must meet in order to generate and store appropriate logs for retention.

SCOPE

This Policy applies to all University IT Systems, onsite or hosted that store or process information classified as Protected, Restricted or Reserved under the University InformationSecurity Framework.

This Policy applies to any system, associated with the above scope statement that accepts network connections, provides application hosting or makes access control (authentication and authorization) decisions.

This Policy is limited to system logging and does NOT cover Data Protection, Monitoring or Interception.

GENERAL REQUIREMENTS

All systems within scope must record and retain logging information.

Typical systems would include; Windows, Linux, Unix and VMware Servers, associated Mail, Database and Applications, Workstations, Anti-Malware, Active Directory, Radius, DNS, DHCP,VPN, Firewall, Networking and Telecoms equipment.

The log information should be sufficient to answer the following types of questions:

What?

- Type of event;
- Severity of event e.g. {0=emergency, fatal, error, warning, info, debug, trace};
- Security relevant event flag (if the logs contain non-security event data too);
- Description;

When?

- Log date and time (International format ISO 8601) YYYY-MM-DDThh:mm:ss.sTZD;
- Event date and time - the event time stamp may be different to the time of logging;

Who?

- Source address e.g. user's device/machine identifier, user's IP address, MACaddress;
- User identity (if authenticated or otherwise known);

Where?

- Application identifier e.g. name and version;
- Application address e.g. cluster/host name or server IPv4 or IPv6 address and portnumber, workstation identity, local device identifier;
- Service e.g. name and protocol;
- Window/form/page e.g. entry point URL and HTTP method for a web application,dialogue box name;
- Code location e.g. script name, module name;

Each system must synchronize its time clock with a reputable clock source and where feasible,the University NTP clock source (in.pool.ntp.org) to ensure log events from different systems can be correlated. Co-ordinated Universal Time (UTC) is the standard strongly preferred.

All administration level access to each system must use accounts, which identify individual administrators or system processes. Generic or default accounts shared by multiple administrators or processes should not be used.

The logs generated from each system must provide enough information to be useful for the IT Security team and the IT System or application owners.

Access permissions to local and central logs must be managed such that unauthorized users cannot modify or interrupt the processes used to create or store log files on systems.

Log files stored in the central logging system must be set to restrict access privileges for eachset of system logs, to authorized accounts and users.

ACTIVITIES TO BE LOGGED

IT system and application owners are expected to assess if systems falling into their areas of responsibility are in scope.

Logs must be set to capture security and event information as a minimum. If feasible, log information must be created whenever any of the following activities are performed by the system:

- Create, read, update, or delete information, including confidential authenticationinformation such as passwords;
- Initiate or accept a network connection;
- User authentication and authorization, such as user login and logout;
- Password resets and credential recovery mechanisms such as those used in Web SSO;
- Grant, modify, or revoke access rights, adding a new user or group, changing user privilege levels, file permissions, database object permissions and firewall rules;
- Configuration changes, including installation of software patches and updates,
- Application process start-up, shutdown, or restart;
- Application process abort, failure, or abnormal end, resource limit or threshold (i.e.CPU, memory, disk space), failure of network services such as DHCP or DNS, or hardware fault;
- Unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database

- Detection of suspicious / malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-malware system.

FORMATTING, TRANSMISSION AND STORAGE

The IT system must support the formatting and storage of logs in such a way as to ensure theintegrity of the logs and to support enterprise-level analysis and reporting. Mechanisms known to support these goals include but are not limited to the following:

- Operating system event logs;
- Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols;
- Logs stored in an ANSI “standards based” SQL database that itself generates auditlogs in compliance with the requirements of this document;

In addition to logs, which are held locally by each system, the log information required by thisPolicy must be passed simultaneously to the IT Services Central Log Store.

Where possible, any data transmitted between log sources and a centralized log store must be secured to prevent unauthorized modifications. Those devices and log agents not supporting encrypted communication channels natively and using plaintext protocols can beprotected with additional layers of encryption such as Internet Protocol Security (IPsec) tunnels.

For log data sent to the centralized location, security measures such as digital signing or encryption should be implemented to ensure the integrity of this data, although for large volumes this may have unacceptable efficiency or administrative overheads and an exceptionwill need to be requested.

Local, system storage must be managed by the system owner to ensure enough capacity hasbeen assigned for the raw log file retention period to be 6 months or for as long as is feasible.

RETENTION

All logs required by this policy and where feasible must be retained for a minimum of 90 days.

Any logs related to this Policy and which contain Personal Data as defined by the University Data Protection Policy, must not be retained for longer than 12 months.

POLICY COMPLIANCE

It is accepted that full Policy compliance across the institution may take some time and require a phased approach, however it is expected that all relevant IT systems, in all departments will comply.

Priority will be determined on the classification of data held within each system, the usefulness of the log data to the IT Security team, and then the feasibility of collecting such log data.

The IT Security and Information Security teams will verify the resultant compliance to this policy through various methods, including but not limited to, system native log data requests,central logging service analysis, business tool reports, internal and external audits, and feedback to the policy owner.

REVA UNIVERSITY

Bengaluru, India

Rukmini Knowledge Park, Kattigenahalli
Yelahanka, Bengaluru - 560 064
Karnataka, India.

Ph: +91- 90211 90211, +91 80 4696 6966
E-mail: admissions@reva.edu.in

Follow us on

/REVA University

www.reva.edu.in