Appendix C

E-Mail Security and Etiquettes and Policy Template for Computer and Network Usage

Introduction

This appendix has two parts:

Part I discusses about etiquettes and security for electronic mails.

Part II discusses about Computer and Network Usage Policy template.

Use this appendix in reference to Chapters 2, 4 and 10 of the book. Security threats, arising from careless use of electronic mails (E-Mails), are explained in Chapters 2 and 4. In Section 9.3.1 (Overview of Web-Threats to Organizations), Chapter 9, Spam mails were mentioned in the context of web threats. Fake E-Mail threats are mentioned in Box 2.7 in Chapter 2. It was explained how E-Mail attachments are used by cybercriminals to send Malicious Code. It is mentioned in Chapter 4 that hand-held devices such as the personal digital assistants (PDAs) allow individuals to access calendars, E-Mail addresses and phone number lists and the Internet. In view of this, due care should be taken while making use of E-Mail technology that is now the most common method of communication among individuals and among organizations.

Part I: Ethics and Security for Electronic Mails

C.1 Security Threats Posed by Electronic Mails

Two principal components, mail servers and mail clients, support E-Mail processes. The mail server is the computer host that delivers, forwards and stores mails. Users interface with the mail client software to read, compose, send and store E-Mail messages. As they are vulnerable targets for attack by malicious intruders, both mail servers and mail clients must be protected. After web servers, an organization’s mail servers are typically the most frequent targets of attack as both mail servers and public web servers communicate to some degree with unknown parties, who may or may not be trustworthy. Attackers, with their thorough understanding of the supporting computing and networking technologies, have been successful in exploiting weaknesses in mail servers and clients. Mail servers and clients can be vulnerable to events such as:

1. Denial-of-service (DoS) attacks that are directed to the mail server or its supporting network which can deny or hinder access to the mail server by valid users.
2. Sensitive information on the mail server may be disclosed or changed in an unauthorized manner.
3. Sensitive information that is transmitted unencrypted between mail server and E-Mail client may be intercepted. For example, the E-Mail software may default to sending usernames, passwords and the E-Mail message itself without the protection of encryption.

4. Information within the E-Mail message may be altered at some point between the sender and the recipient.
5. A successful attack on a mail server can be used to gain unauthorized access to resources elsewhere in the organization's computer network, including user passwords and other computers on the network.
6. A mail server that has been attacked can be used to attack another organization's network, perhaps creating liability for damages to the sending organization.
7. Attackers may use the organization's mail server to send E-Mail-based advertisements (commonly referred to as Spam).
8. Viruses and other types of Malicious Code may be disseminated to computers throughout an organization via E-Mail.
9. Users may send inapt, private or other sensitive information via E-Mail. This could expose the organization to lawful actions.

The main objectives of E-Mail security are to ensure the following:

1. Non-repudiation, that is, sender cannot deny sending the message at a later date, and the receiver cannot deny receiving it.
2. Messages are read-only by their intended recipients integrity of the message.
3. Authentication of the source (i.e., the sender or senders' network).
4. Verification of delivery.
5. Labeling of sensitive material.
6. Control of access (to E-Mails).

C.2 Countermeasures to Protect from Threats Posed through E-Mails

E-Mail may be the most heavily used feature of the Internet or LANs in an organization; however, if not managed, it could be dangerous for a number of reasons: (a) Attachments containing viruses can be sent (see Box C.1) and (b) through passive attacks, data packets can be "sniffed" to learn about the IP addresses of corporate networks, etc. In the face of this, organizations need to take countermeasures to minimize the damage for threats posted through E-Mails. In this section we discuss this.

Box C.1: KRESV Test – Be Careful When Reading E-Mail with Attachments!!

You probably receive lots of mails each day. Most of it may be unsolicited (unsolicited mails are referred to as "Spam") and may contain unfamiliar but plausible return addresses. The senders are trying to support you to open the letter, read its contents, and interact with them in some way that is financially beneficial to them. Even today, many of us open letters to learn what we have won or what fantastic deal awaits us.

Viruses and worms that come through E-Mails operate much the same way, except that there are consequences, sometimes significant ones. Malicious E-Mail often contains a return address of someone we know and often has a provocative subject line. This is social engineering at its finest – something we want to read from someone we know. E-Mail viruses and worms are common. If you have not received one, chances are you will. Here are steps you can use to help you to decide what to do with every E-Mail message with an attachment that you receive. You should only read a message that passes all of these tests**:**

1. **The know test:** Is the E-Mail from someone that you know? Are you sure about the source?
2. **The received test:** Have you got an E-Mail from this sender previously?
3. **The expect test:** Did you expect E-mail with an attachment from this sender?

4. **The sense test:** Does the E-Mail from the sender have the text as described in the subject line and does the name of the attachment(s) make sense? For example, would you expect the sender – let's say your mother – to send you an E-Mail message with the subject line "Here you have, ;o)" that contains a note with attachment – let's say AnnaKournikova.jpg.vbs? A message like that probably doesn't make sense. In fact, it happens to be an instance of the Anna Kournikova worm, and reading it can harm your system.
5. **The virus test**: Does this E-Mail have a virus? To decide this, you need to install and use an antivirus program.

You should apply these five **KRESV** as mentioned above to every piece of E-Mail with an attachment that you receive. If any test fails, toss that E-Mail. If they all pass, you still need to use care and look for surprising results as you read it.

A few countermeasures, to minimize threats from E-Mails, are listed below.

Countermeasure No. 1: Careful Planning to Address the Security Aspects of Mail

Server Deployment

All mail server activities should be carried out in compliance with the organization's plans and policies. Plans and policies should support the application of consistent management controls across the entire organization. This is essential to avoid variations in controls that can result when the information technology support staff becomes fragmented within the organization. When planning a mail server, the following items should be considered:

1. Identify the purpose of the mail server and the information to be processed on or transmitted through the mail server.
2. Identify the security requirements of the information.
3. Identify other services to be provided by the mail server and their security requirements.
4. Identify the location of the mail server, the network services to be provided, and the network service software on both the clients and the server.
5. Identify the users or categories of users of the mail server and any support hosts.
6. Decide the privileges that each type of user will have on the mail server and support hosts.
7. Consider issues such as authentication methods, enforcement of access rules, cost and compatibility with the existing infrastructure, employee skills and vulnerabilities.
8. Work closely with vendors in the planning stage.

Countermeasure No. 2: Security Management Practices and Controls for Securing Operation of the Mail Server

Protecting the operating system helps to protect the mail server from exposure to danger. Suitable management practices are necessary to operate and maintain a secure mail server. Security practices include the identification of an organization's information system assets and the development, documentation and implementation of policies, standards, procedures and guidelines. The objective is to make sure that the *confidentiality*, *integrity* and *availability* of information system resources are in place.

Countermeasure No. 3: Deploying, Configuring and Managing the Mail Server to Meet the Security Requirements of the Organization

The operating system that supports the mail servers must be secured. It is important to check the hardware and software configurations, which may have been set originally to emphasize features, functions and ease of use, rather than just the security of the system. As each organization has unique security needs, the mail server administrator should configure new servers to meet the organization's requirements. As requirements change, systems should be reconfigured. To secure the operating system, following steps should be followed:

1. Patch and upgrade the operating system to correct known vulnerabilities.
2. Remove or disable all unnecessary services and applications, and enable only those services that are required by the mail server.
3. Configure the operating system to authenticate users.
4. Configure access controls to specify access privileges to files, directories, devices and other resources.
5. Test the security of the operating system periodically to identify vulnerabilities and to validate the effectiveness of security measures.

Countermeasure No. 4: Making the Mail Server Application Compliant with Security Requirements of the Organization

In general, the same steps, which are recommended for protecting the operating system, are also applicable to secure installation and configuration of the mail server application. The goal is to install the minimal amount of mail server services required and to eliminate any known vulnerabilities through patches or upgrades. The following steps are worth considering securing the mail server application:

1. Patch and upgrade the mail server application to correct for any known vulnerabilities.
2. Remove or disable unnecessary services, scripts, applications and sample content.
3. Configure mail servers to require authentication of users.
4. Configure mail servers to implement the same or more restrictive controls on access to resources as those enforced by the operating system.
5. Test the security of the mail server application.

Countermeasure No. 5: Using Cryptography to Protect User Authentication and Mail Data

Cryptographic functions can be added to standard E-Mail protocols to allow for encryption of the message, authentication of sending party, non-repudiation of the message and integrity of the message (see Box C.2). Mail protocols can be attacked when they default to unencrypted user authentication and when they are used to send E-Mail data in the clear (i.e., unencrypted) text. Attackers can intercept this data, compromise a user's account and alter unencrypted messages.

At a minimum, organizations should consider encrypting the user authentication information even if they do not encrypt the E-Mail message. Encrypted user authentication is now supported by most standard and proprietary mailbox protocols. There are many issues to consider for encryption of E-Mail. Encrypting E-Mail places a greater load on the user's computer and on the organization's network infrastructure. Encryption may complicate virus scanning and mail content filtering, and usually entails significant administrative overhead. However, for many organizations, the benefits of E-Mail encryption will prevail over the costs.

Box C.2: Message Integrity

Cryptography can detect if an E-Mail message has been modified in an unauthorized manner. It can do this in a couple of ways. The first way is that message will usually not decrypt properly if parts of it have been changed. The other way is through *parity bits.* A parity bit is a binary digit that indicates whether the number of bits with value 1 in a given set of bits is even or odd. Parity bits are used as the simplest error detecting code.

Parity checking is the most basic form of error detection in communications. Parity bits have been used in different protocols to detect modification of streams of bits as they pass through one computer to another. However, parity bits can usually be only detected in unintentional modifications. Unintentional modifications can happen if there is a spike in the power supply, if there is interference attenuation on a wire or if some other type of physical condition occurs resulting in corruption of bits as they travel from one destination to another (recall the sequence of events described to explain what happens when the user clicks the “send” button of E-Mail).

Parity bits cannot be identified if a message was captured by an intruder, altered (deliberately), and then sent on to the intended destination. This is because the clever intruder can just recalculate a new parity value that includes the changes made and the receiver (data transmission equipment at the receiver end) would not the difference. Cryptography turns out to be the superior method in situations like these.

For readers interested in understanding more about parity bit and parity checking, Internet resources have been mentioned in Ref. #1, Additional Useful Web References, Further Reading.

Countermeasure No. 6: Use of Network Infrastructure to Protect the Mail Servers

The network infrastructure, including the firewalls, routers and intrusion detection system that support the mail server, plays a critical role in maintaining the security of the mail server. In most configurations, the network infrastructure is the first line of defense between potential attackers using the Internet and the mail server. Network design alone, however, cannot protect a mail server. Attacks have been too frequent, sophisticated and varied. The best defense is through the application of diverse and layered protection mechanisms.

Countermeasure No. 7: Ongoing Maintenance Mail Server Security

Maintaining a secured mail server requires continued effort, resources and vigilance from an organization. Daily attention to the administration of a mail server is essential. The following steps are recommended for maintaining the security of mail servers:

1. Configure, protect and analyze the log files of information about access and use of the mail server.
2. Back up the data on the mail server frequently.
3. Analyze intrusions and protect against Malicious Code (e.g., viruses, worms, Trojan Horses) – remember the discussion in Chapters 2 and 4.
4. Establish and follow procedures for recovering from security compromise – recall the discussion in Chapter 9 about security incident handling (Section 9.9).
5. Test and apply patches in a timely manner.
6. Test the security of the system periodically.
7. Analyze intrusions and protection against Malicious Code (e.g., viruses, worms, Trojan Horses). Recall that viruses, worms and Trojan Horses are explained in Chapters 2 and 4.
8. Establish and follow procedures for recovering from security/privacy compromise.
9. Test and apply patches in a timely manner.
10. Test the security of the system periodically.

C.3 Governance for Electronic Mail Systems

The discussion about security threats posed by E-Mails to information systems prompts us for the need for establishing E-Mail governance. Governance consists of policy, procedures, standards and controls. E-Mail messages are frequently used as substitutes for telephone. At the same time, people use E-Mail systems to communicate substantive information previously committed to paper and transmitted by traditional methods. This interesting combination of communication and records keeping has created ambiguities on the status of E-Mail messages. Laws of countries hold position on the interpretation of electronic evidence (refer to Appendix Q – Indian Evidence Act).

C.4 Standards for Securing Electronic Mail

Standards are critical to the successful exchange of E-Mail. Standards for E-Mail have been developed by the *Internet Engineering Task Force* (IETF), a large open international community of network designers, operators, vendors and researchers, who are concerned with the evolution and operation of the Internet architecture. The standards cover the composition, formatting, transmission, delivery and storage of E-Mail.

Earlier in this appendix, it was mentioned that the main objectives of E-Mail security are to ensure non-repudiation, messages reaching only their intended recipients, integrity of the message, authentication of the source, verification of mail delivery, labeling of sensitive material and controlled access to E-Mails. There are some “standards” developed to address some or all of the security issues mentioned above, which are as follows:

1. **Secure multi-purpose Internet mail extensions (S/MIME):** This is a specification that adds security services to E-Mails. It follows the Public-Key Cryptography Standards (PKCS).
2. **MIME object security services (MOSS):** Introduced in 1995, this standard provides flexible E-Mail security services by supporting different trust models.
3. **Privacy enhanced mail (PEM):** PEM is a standard that was proposed by the IETF to be compliant with the Public-Key Cryptography Standards (PKCS), which was developed by a consortium that included Microsoft, Novell and Sun Microsystems.
4. **Pretty Good Privacy (PGP):** “Pretty Good Privacy” is a software which encrypts your E-Mail as well as digitally “signs” it so that you don’t have to worry about forgery. PGP is available on many platforms, including DOS, Windows, OS/2, MacOS and most UNIX variants.

C.5 Conditions/Rules for E-Mail Access

Organizations should exercise extreme care while granting access to their E-Mail systems (refer to the discussion about access management in Chapter 9, Section 9.3.1, subsection “Challenges in Controlling Access to Web Applications”). Depending on the nature of the information being exchanged through E-Mail, the policy governing access by third parties should be as unintrusive as possible. At a minimum, the policy should require that, if possible, a request for access to E-Mail messages be made directly to the employee. For example, employees could be reached on their phone contact number at home or could be asked for access to their E-Mail prior to going on a vacation. When it is not possible to obtain access to E-Mail straight from the employee, the policy should limit access by third parties for legitimate business purposes, when there are no other readily available means to obtain the information.

From a privacy standpoint, there is a difference between non-confidential work-related messages on one hand and confidential or personal communications on the other. In order to guard the user’s privacy, wherever possible, the two types of communications should be stored separately. This would allow personal communications to be password-protected and kept in a storage area that cannot be readily accessed by others. In the event that there is a need to search an employee’s non-confidential work-related E-Mail messages, the threat to the employee’s privacy would be minimized.

C.6 Retaining Records from an E-Mail System

In the previous section, we learned about retaining privacy and protection concerning E-Mails. In this section, we will learn about E-Mail-based information that may deem to be recorded. Readers will recall the information classification discussed in Chapter 9 (Section 9.11). The management of E-Mail systems touches on nearly all functions which an organization is dependent on – record keeping for privacy, administration, vital records management, administrative security, auditing, access and archives. The need to manage E-Mail systems properly, then, is the same as for other record-keeping systems to ensure compliance with statutes concerning the creation of, retention of and access to records. Especially, from audit perspective and transaction tracing point of view, the discussion below is important.

Organizations need to explore three options while retaining records from an E-Mail system:

1. Online storage.
2. Near-line storage.
3. Offline storage.

Each of these alternatives carries with it advantages and disadvantages and may be affected by organization's widespread information technology environment. Where personal communications are stored independently from work-related communications, the policy on access to personal communications can be more restrictive. For example, the right to use personal communications on behalf of third parties could be prohibited. On the other hand, the policy may limit access to those situations which are sufficiently urgent to warrant the loss of privacy associated with read to an employee's personal E-Mail messages. A more restraining policy would limit access to circumstances where violations of policy or security are suspected, or for law enforcement purposes. With E-Mail systems, three kinds of storages come into picture; they are explained as follows:

1. **Online storage:** It is defined as storage of E-Mail messages, metadata and attachments in an E-Mail system which is being used at an agency. This type of storage has complete features of the E-Mail message, and allows users to recall the message at any time for reference or responding. The downside of online storage includes the impending costs and effects of storage on the performance of the E-Mail system. Any solution for retaining E-Mail includes online storage and that should be done only in discussion with organization's information resource manager and the agency network administrator.
2. **Near-line storage:** This is defined as storage of E-Mail messages, metadata and attachments in an electronic record-keeping system. For this type of storage, it is required that the message, metadata and attachments be detached from the online E-Mail system and stored in an electronic format. For example, a message stored in an online E-Mail system can be saved to a file on a local hard drive. The file should be stored in a format which is compatible with agency operations and filed according to filing practices established by the agency and/or user. Near-line storage allows the user to maintain a reasonable level of functionality, in that E-Mail messages stored near-line can be retrieved and referenced electronically. In storing E-Mail messages, metadata and attachments, users should be careful to maintain a filing system which is consistent with established practices. This includes filing sequences as well as the use of naming conventions for computer files. In addition, users may want to consider "protecting" such records from alteration.
3. **Offline storage:** This is defined as the storage of E-Mail messages, metadata and attachments outside of an electronic record-keeping environment. The finest example of this type of storage is to simply print out an E-Mail message to paper, with its contextual information and attachments in place, for filing within existing filing systems in the agency. Offline storage radically reduces the functionality, in the sense that E-Mail messages can no longer be retried in electronic form. At the same time, offline storage does offer to users the facility to integrate the filing of records in E-Mail systems using existing hard-copy filing systems. Any E-Mail messages, metadata and attachments stored offline should be done in a manner consistent with agency practice.

In addition to standards and procedures for storing records and evidences that originate from E-Mail, organizations need to establish sound policies for use of E-Mails in the organization. In Box C.3, we provided one such example from a hypothetical university.

Box C.3: Electronic Mail Systems Policy – An Example

Purpose
To outline the standards and guidelines to be followed with regard to the security and use of E-Mail systems.

Standard (rules for E-Mail usage)
XYZ University's E-Mail systems are University assets, which must be used for University’s official work only. Incidental and occasional personal use of E-Mail is permitted, however, must not be abused.

Individuals should be made aware that messages sent over E-Mail systems are subject to monitoring, if such action is deemed appropriate and authorized by senior management. The University reserves the right to access E-Mail messages for the following purposes:

1. To comply with an investigation.
2. To recover from system failures.
3. To investigate suspected breaches of security or violations of policy.

It is a violation of University’s Electronic Mail Policy for any individual to intentionally access another individual’s E-Mail files for unapproved business purposes.

1. E-Mail must not be used for the purpose of chain letters, personal advertisements or solicitations. All E-Mail should be professional and courteous. The use of profanity or offensive language is prohibited.
2. When sending E-Mail, the use of the “everyone” option must be used only for global messages affecting all individuals. The “everyone” option should be restricted to the E-Mail administrator, in most cases. Individuals needing to send messages to all users should submit the message to the E-Mail administrator. It will then be scheduled for distribution.
3. Individuals must use proper judgment when using E-Mail. When sending a confidential or private E-Mail message, individuals should code the message as such to prevent the recipient from forwarding the message to unauthorized or unintended individuals.
4. To improve system performance and conserve system resources, the University reserves the right to periodically delete stored messages.

C.7 E-Mail Ethics and Etiquettes: Useful Tips

1. When using the E-Mail facility running at your office, be sure to check with your employer about ownership of E-Mail. Laws about E-Mail may vary from country to country.
2. Unless you are using an encryption device (either hardware or software), it is good to assume that mail on the Internet is not secure. Never put in a mail any kind of message that you would not put on a postcard.
3. Respect the copyright on material you reproduce. Remember that almost every country has copyright laws (see Appendix T – The Indian Copyright Act).
4. When forwarding or re-posting a message you have received, do not change the wording. If the message was a personal message to you and you are reposting to a group, you should ask for permission first. You may shorten the message and quote only relevant parts; however, be sure that you give proper attribution.
5. Never send chain letters via E-Mail. Some organizations may forbid chain letters through E-Mails; your network privilege may be revoked if you do not abide by these rules. Notify your local system administrator if you ever receive a chain mail.
6. Be “conservative” in what you send and be “liberal” in what you receive; this is a simple rule of thumb!
7. Check all your mail subjects before responding to a message. Also make sure that the message you respond to was indeed directed to you; you might be copied rather than being the primary recipient.

8. When required, always include your contact details in your mail closing information; many mailers strip header information.
9. Mail should have a subject heading which aptly but precisely gives an idea about the mail content.
10. There are addresses which may go to a group but the address looks like it is just one person; so be careful when addressing mail.
11. Watch "CCs" when replying; do not continue to include people if the messages have become a two-way conversation.
12. Be aware that you could be sending messages across the globe; so be sensitive to the geographic time zones.
13. Verify all addresses before initiating long or personal response; general rule is that any electronic message containing over 100 lines is considered "long." It is a good idea to include this word in the mail header to warn the receiver that s/he is going to deal with a long mail!
14. Use mixed case; UPPER CASE GIVES A FEELING YOU ARE SHOUTING!
15. Use symbols for emphasis where required, for example, That *is* what I mean.
16. Use smileys to indicate the tone of voice but use them sparingly :-).
17. Use FLAME's carefully and judiciously – flames, question marks, etc. are various symbols – allowed in some mail systems; for example, the Lotus Mail system.
18. If you send encoded messages, make sure your recipient can decode them.
19. Never send large amount of unsolicited information to people.
20. Be careful with the attachments you send because depending on the rules in place for mail sizes for delivery, your mail may not get delivered or may use excessive resources of the E-Mail system if the attachment included is too large. In general, it may not be good to send anything larger than 50 KB, but again it would depend on the particular E-Mail system you are using and the rules in place in the organization.
21. Last but not the least, be careful on the mail forwarding message. Be sure you have not set forwarding on several hosts so that a message sent to you gets into an endless loop from one computer to the next to the next!

Part II: Computer and Network Usage Policy Template

Refer to the discussion in Section 9.8.1 of Chapter 9. In this section of the appendix, we provide an example template in the context of discussion in Section 9.8.1. You may adopt this template for your use; however, you may need to make appropriate modifications to suit your circumstances. This is only a template to provide an example. This example is based on an academic institution scenario. The university name mentioned in this template is hypothetical; any resemblance with real-life institution is purely accidental and not intentional. Wherever dates are mentioned as <ddmmyy>, they are supposed to be only indicative; the "ddmmyy" notation simply means that when the template is used, real dates as applicable can be mentioned. All the website links mentioned (you will see them on following pages) are also hypothetical; any resemblance or co-incidence that may be found with real-life websites is purely accidental.

- **I.** Introduction.
- **II.** Definitions.
- **III.** Use and authorization.
- **IV.** Limitations/restrictions on users' rights.
- **V.** Services.
  - **A.** Academic/administrative and remote usage network.
  - **B.** E-Mail.
  - **C.** LISTING Service
  - **D.** The University website.
  - **E.** Learning and knowledge management system.
  - **F.** Virtual Private Network (VPN).
  - **G.** Unauthorized use.

I. Introduction

Shree Vidya University (hereinafter also referred to as “University”) sees itself as a global institute for learning. Access to information technology (IT) constitutes an important element in University’s mission of imparting knowledge and services to our students, faculty and staff. The use IT (information technology) is considered to be an essential element in the delivery of educational services with the highest quality. The quest for and attainment of the mission of education, research and public service means that the opportunity of using computing systems and software, internal and external data and networks, as well as access to the World Wide Web (WWW) should be made available to the community connected with this university. The safeguarding of that privilege for the full community needs that each faculty and staff member, student and other authorized user abide by institutional and external standards for suitable use.

To assist and to ensure such compliance, Shree Vidya University establishes the following policy that supplements all applicable university policies, including gender harassment, patent and copyright, and student and employee punitive policies, as well as applicable laws.

II. Definitions/Explanations (Alphabetically Organized)

Following are a few explanations or definitions for terms given in alphabetical order:

1. **Authentication credentials:** Assigned User ID/username and PIN/password (changed by users) that, used in conjunction, authenticates users to privileged computing facilities and resources.
2. **Computing facilities:** All software applications, mainframes, desktop and mobile computers, networks and computer peripherals licensed, owned or operated by this university.
3. **Course list:** Refers to the dedicated list created upon request for the purpose of communicating between students registered for a particular course and section and the faculty member teaching the course.
4. **Departmental (Majors) list:** Refers to a list created (when requested) for a department to communicate with students in their major.
5. **DSL:** Digital Subscriber Line (DSL) is a type of high-speed Internet access. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
6. **E-Services:** University’s terminology relating to electronic services such as E-Mail, learning management system and electronic library resources.
7. **Internet:** All networks external to this university.
8. **Intranet:** All networks internal to the university.
9. **List conduct:** Refers to the behavior of a list subscriber in the context of the list as reflected by the subscriber's postings.
10. **List content:** Refers to the theme, topic or purpose of the list as declared on the list application and/or the theme, topic or purpose of list postings.
11. **LISTING Service Manager:** The Information Technology Services’ (ITS) designated manager of the LISTING Service.
12. **List owner:** Refers to a person (other than the LISTING Service Manager) who has administrative rights to the list. This may or may not be the list sponsor.
13. **List sponsor:** The LISTING Service list applicant (the person who submits the application as designated in list 2) assumes overall responsibility for and ownership of the list of applications.
14. **Managed:** Software and antivirus upgrades that are controlled by a server and “pushed” to the desktop.

15. **Remote access:** Any access to university's administrative network through a non-university controlled network, device or medium.
16. **Unmanaged:** A device used for computing that does not have antivirus definitions or upgrades installed on it automatically. The user of the computing device (i.e., computers, etc.) installs all upgrades manually.
17. **Users:** Individuals who use university's facilities for computing. Most users are students, faculty and staff members of this university. Some users could be external personnel who are authorized by campus authorities to avail computing facilities. For example, some such users could be volunteers for local non-profit agencies, scholars visiting from other institutions, associated with the university and the like.
18. **Virtual Private Network (VPN):** A way to extend the corporate/production (trusted) network using authentication and encryption.

III. Use and Authorization

A. Authorized Activities

University's computer facilities are a resource for members of the campus community (faculty, staff, students and other affiliated individuals or organizations authorized by this university) to be used for work consistent with the instructional, research and administrative goals of the university as defined in the university's "Missions and Goals" statement.

Use by non-allied institutions and organizations shall be in accordance with University's Administrative Procedures Manual Policy 005-A: Use of Computer Equipment or Services by Non-allied Institutions and Organizations. All who use university's computer facilities have the accountability to do so in an effective, efficient, ethical and legal manner, as mentioned below.

B. User Accounts

Shree Vidya University provides access to particular computer systems with the obligation of specific user accounts based on educational and business need for access. Every computer user account issued by this university is the responsibility of the person in whose name it is issued. University-accepted clubs and student organizations may be issued a user account. Faculty advisors shall assign a particular person or persons authorized to act on behalf of the club or organization. This person(s) is in charge of all activity on the account and will be subject to university disciplinary procedures in case of misuse. Such misuse situations include, but are not limited to, examples of theft of services, and they will have the associated penalties described in Section IV.

1. Acquiring a username in another person's name.
2. Use of a username without the explicit authorization of the account owner and without the permission obtained from ITS.
3. Allowing others to use your username without explicit permission obtained from ITS.

C. Password Security

It is compulsory that user accounts be kept safe by using strong passwords, keeping passwords secret and changing the passwords often. Users must select a password in a way that will protect their account from illegal use, and which will not be cracked easily. Do not select passwords that can be easily guessed, for example, nicknames, birthdates and telephone numbers. Users must notify ITS about any use of a user account without the clear permissions of the owner and ITS.

D. User Privacy

This university does not generally monitor or control the objects residing on state-owned or non-state-owned electronic devices, whether or not such devices are linked to the campus networks. However, devices that are utilized in violation of university's policies are subject to inquiry and termination of connection without issuing prior notice.

No user should view, copy, modify or wipe out another individual’s personal or state-owned electronic files without permission (unless authorized or required to do so by law or regulation). University’s computing and network resources are designed to safeguard user privacy; users shall not attempt to evade these protections. University reserves the right to access all aspects of its computing and network resources, together with individual usage to decide if a user is violating this policy or state or other national laws.

E. System Integrity and Denial of Service

Users shall value the system integrity of campus computing facilities. For example, users shall not deliberately build up or use programs that penetrate a computing system, or harm or modify the software components of a computing or network system.

F. Resource Accounting

Users shall not develop or use procedures to modify or evade the accounting and monitoring of the use of computing facilities. For example, users may not make use of computing facilities incognito or by means of an alias, and may not send messages, E-Mail or print files that do not display the correct username of the user performing the operation.

G. Use of Computing Resources

Computing hardware at Shree Vidya University is meant to be used for academic and business purposes. All equipment is tagged with university’s asset tags and is registered into the inventory annually. Any information stored, processed or transmitted by university computer may be monitored, used or disclosed by official personnel, including law enforcement. Computing facilities at university offices and laboratories ought to be used in a responsible and disciplined manner. Users shall not develop or use procedures that hinder official use by others. Users shall not meddle with computer setups which are meant to keep computer software up to date and legal, and shall not install personal software. Users shall not use applications that utilize an uncommonly high portion of the network bandwidth. Users shall avoid wasting computing resources by too much game playing or other insignificant applications; by sending chain letters or other frivolous or excessive messages locally or over the network or by printing too many copies of documents, files, images or data. Printing facilities provided on campus must be used only for academic work, intellectual growth or administrative business.

H. Licenses and Copyrights

Users shall not breach the legal protection provided by copyrights and licenses held by the university. Users are not allowed to make copies of any licensed or copyrighted computer program residing on any of Shree Vidya University’s computer or storage device without obtaining an official permission from ITS. Prevailing copyright law grants authors certain selected rights for copying, adapting, sharing, displaying, attribution and integrity to their creations. Literary works, photographs, musical work, software, films and artifacts in video form can all be copyrighted. A few examples of potential copyright law violations include, but are not limited to, creating unauthorized copies of any copyrighted material (such as commercial software, text, audio and video recordings, graphic images, etc.); disseminating copyrighted materials through computer networks or through other means; selling data or programs residing on campus computers, or using them for commercial purposes or for personal financial gain; or public leak of information about computer programs (e.g., source code) without seeking owner’s explicit permission.

I. System Access Restrictions

Access to certain administrative computers and programs at Shree Vidya University campus is restricted. Such accesses are granted only on a “need-to-know” basis in line with university’s access control policy guidelines. Unofficial access, spoofed access or any illegal attempts to access to data/program on Shree Vidya University’s special class computing systems/computers will be treated as “theft” and such acts will be subject to the penalties described in Section IV (Limitations on Users’ Rights) of this document. Official permission for use of these systems is decided solely by ITS, on behalf of the University Dean, and after review and recommendation by the campus Security Administrator.

J. Recreational Use

Use of university’s computing facilities (including computer games and social network communication) for leisure is permitted only when no other instructional, research or administrative function requires the use of these computing resources for priority use. Individuals who use university computers for recreational purposes are required to surrender the computer immediately to persons who need it for academic or administrative purposes or other high priority use in connection with Shree Vidya Univesity’s official work.

K. Termination of Access to University’s Computing Facilities

Deliberate breach of policies mentioned in this document will result in instant annihilation of access. Access will also be terminated for:

1. Complete withdrawal by student from university courses.
2. Current students, 90 days after graduation.
3. Faculty/staff, 30 days after termination of employment with the university.

Emeritus faculty and staff retain eligibility for use of university’s computing facilities.

IV. Limitations on Users’ Rights

The password or other means of access, issued to users, is to ensure proper confidentiality of university’s files and information and does not guarantee privacy for personal or improper use of university equipment or facilities. The university provides logical security against intrusion and damage to files stored on central facilities.

University also provides some facilities for archival and retrieval of files as per specifications from users and for recovering files after accidental loss of data. Shree Vidya University is not accountable for unlawful access by other users or for loss due to power failure, fire, floods, etc. The university makes no warranties with regard to Internet services, and it specifically assumes no responsibilities for the content of any advice or information received by a user through the use of university’s computer network.

Users should be aware that university computer systems and networks may be subject to unauthorized access or tampering. Additionally, computer reports, E-Mail, etc. are treated as “records” which may be made easily available to the public under the provisions of the prevailing Information Law.

V. Services

A. Academic/Administrative and Remote Usage Network

Antivirus Protection

It is mandatory to run latest versions of antivirus protection software on very computer connected to the campus network. “Managed” antivirus protection, provided by ITS, will be installed on the majority of campus-owned personal computers. ITS also provides antivirus protection software for use by students. Remote Network (RemoteNet) students may utilize a “managed” or “unmanaged” mode, as owners prefer and as operating systems allow. Non-RemoteNet student antivirus protection is unmanaged.

“Unmanaged” users, who wish to use campus network for connectivity, are responsible to ensure that the antivirus protection used by them is kept up-to-date. These “unmanaged” users would typically include but are not limited to what is mentioned below:

1. Campus-owned Apple-Macintosh, Windows, Linux and UNIX-based machines.
2. Non-campus-owned computers.

3. Computers/notebooks owned by students – for those not wishing to utilize the managed antivirus protection provided by the ITS office on campus.

In addition, outbound RemoteNet E-Mail will be filtered through a server that will scan and detect viruses. ITS and RemoteNet have the authority to disconnect computers from the network that have been detected as infected. The computer system will stay disengaged awaiting the user to show the following:

1. That the machine has been cleaned of viruses/worms.
2. That a suitable antivirus solution has been licensed for the machine throughout the current academic year.
3. That the product has been installed and set up to automatically monitor and install virus discovery updates.

Later infractions resulting due to not having an installed, licensed antivirus product may attract additional penalties.

Desktop Upgrades

Computer systems, connected to the campus network, will have specified operating systems upgraded or patched by a managed service as applicable. "Unmanaged" clients, who wish to use the campus network connectivity, will be responsible for keeping up-to-date all operating systems running on their machines.

Network Use

Users shall not make use of the campus network to provide Internet access to any outside source, be it commercial or private. All RemoteNet (residential) network users must sign off that they have read this University Computer and Network Usage Policy before they are permitted access to the network. Actions harmful or unsuitable while accessing the resources of the university and Internet are listed below only as examples; the list below is not an exhaustive one:

1. **Network naming conventions:** All student users must use the username assigned by the university ("abcd1234") for the computer name that will be displayed on the network. The description field is required to be left blank.
2. **Shared connections:** A network connection supplied by the university is solely for the use of the individual subscriber assigned to that connection. Connections may not be shared among multiple users. No network subscribers shall use any hardware or software mechanisms to offer network connectivity to non-subscribers. Users shall not utilize the campus network to provide Internet access to any external source, either for commercial or private use. Users are by themselves accountable for all use of their computers and network connections and will be held accountable for any violations that occur involving their computer or network connections.
3. **Network infrastructure:** All additions, movements and changes made to network infrastructure electronics include, but are not limited to, products such as Telecom Repeaters, Hubs, Concentrators, Bridges, Routers, Switches, etc. Such infrastructure elements must be synchronized and installed by Shree Vidya University's ITS staff specially trained for this purpose. Such work undertaken or managed by the ITS staff includes all cabling that is patched into these devices used for providing connectivity. Users are not allowed to extend connectivity (provided Ethernet jacks in the room) by connecting to any network devices such as a Hub, Router, Switch, Wireless Access Point, etc. For example, users are not supposed to use a Hub in their room or office to connect more than two network devices on the network at the same time.
4. **Assigned IP address:** Alterations of any kind to the assigned IP address or related settings, including using an unauthorized IP address, are prohibited. RemoteNet IP addresses are assigned dynamically and users are not permitted to configure static IP addresses, DNS address, etc.

5. **File Sharing:** Users are responsible for the security of the system. All student-shared files must be password-protected. If a user misconfigures the file sharing, others may be able to affect and alter the user's computer. Users are responsible for the content of files that they distribute. Current laws may permit users to be sued for libel, invasion of privacy, software piracy, pornography and other such crimes. The university is not responsible for any loss of data that may occur if users choose to activate file sharing.
6. **Copyright:** Allocation of copyrighted materials such as computer software and music is normally forbidden. There may be exception to this where a part of copyrighted material may be part of the public domain. In accordance with the Copyright Act and prevailing laws in the country for governing Higher Education, university policy forbids the copying, distribution, downloading and uploading of copyrighted materials on any personal or on College computer system or on network. These materials include, but are not limited to, text (including E-Mails and web information), graphics, art, photographs, music, film and software. Violators of the Copyright Act who have illegally shared copyrighted files are subject to civil penalties between Rs. 7,500 and Rs.15,000 per copying crime. Refer to university website for copyright-related procedures.
7. **Monetary gain:** Network access for monetary gain or for business activities of groups or organizations is prohibited. Re-sale of access or services is prohibited.
8. **Domain registration:** The university prohibits the registration of commercial hostnames to a Network IP address.
9. **Servers:** The university does not allow establishing a server or offering a service that over-uses the shared bandwidth. Some examples of server programs are File Transfer Program (FTP), web servers, E-Mail servers, peer-to-peer, etc.
10. **Port scanning:** Scanning for computers on any network using port scanners or network probing software including packet sniffers is prohibited.

The university networks are monitored and violators of university policy will be denied service and referred to the proper authority, as specified in Section V of this policy.

Wireless Network

The wireless network is not meant as a replacement for the wired network and is not to be used as a primary network connection. The wireless network is meant to extend the wired network for simple uses in areas where wired network access is unavailable. Users are supposed to avoid using applications that consume large network bandwidth. These include servers and file-sharing applications. Users should be aware that the university does not utilize 802.11b/g/n encryption standards on the campus wireless network (i.e., WEP, WPA and WPA2).

There are other electronic devices that use the same 2.4 GHz frequency as the university wireless network. Such devices include 2.4 GHz cord-free phones, microwave ovens, X10 wireless cameras, Bluetooth devices and other wireless LAN equipment. Devices operating with this technology can cause sporadic failure and discontinuity of service.

The following policies are in addition to university's campus network usage policies. While accessing the resources of the university and Internet, avoid actions that are harmful or wrong. A partial list of some examples of such actions is indicated as follows:

1. Users may not extend or modify the network in any way. Some examples of such act are installing bridges, adding access points and switches, hubs or telecom repeaters. The university has the right to eliminate or disconnect any unauthorized access points that may be discovered through unauthorized access attempts.
2. Users will be responsible for all costs associated with purchase, installation, operation and support of wireless adapters in client computers.
3. Any attempt to break into or gain unauthorized access to any computers or systems from a wireless connection is prohibited.

4. It is not allowed to run any unofficial data packet collection programs on the wireless network. Such practices will be treated as a breach of privacy and will be considered as attempt to steal user data.
5. The institution has the right to limit bandwidth on a per connection basis on the wireless network, as necessary, to ensure network reliability and fair sharing of network resources for all wireless users.
6. Any attempt to bypass the security systems designed to prevent unauthorized access to the wireless network of Shree Vidya University may result in the termination of all access and may also call for a disciplinary action as deemed appropriate by the university board.
7. Information about the campus wireless network including recommended computing habits and wireless coverage on campus can be accessed at:
   http://www.shreevidyauniversity/its/networking/wireless/

B. Electronic Mail

University Use of Electronic Mail

This university uses E-Mail as the mechanism for official communication. It is the university's expectation that such mail communications will be received and read in a timely manner.

Official University E-Mail Accounts

In the official university E-Mail account, the address has "university.edu." at the end. All students, faculty and staff are assigned an E-Mail address and account. The E-Mail address is directory information. As with other directory information, in compliance with prevailing Privacy Act regulations, any student may request that his/her official E-Mail address be restricted in its access.

Expectations for Use of E-Mail

Faculty, staff as well as students are responsible to use this E-Mail in a well-organized, efficient, courteous, right and legitimate manner. The university expects students, faculty and staff to check their E-Mail regularly in order to stay current with university-related communications. Department heads who have exempted employees from the requirement of having an official E-Mail account must make arrangements for alternative methods of access to official communications. Students have the accountability to understand that some communications may be time-critical. Excuses such as "I did not/could not check my E-Mail," "there was error in forwarding mail," or E-Mail returned to the university with "Mailbox Full" or "User Unknown" are not good enough excuses for not having noted official university communications via E-Mail.

Redirecting of E-Mail

If a student, faculty or staff member needs to forward E-Mail from their official @shreevidyauniversity.edu address to another E-Mail address (e.g., @gmail.com, @hotmail.com), they may do so, but by their own initiative and at their own risk. The university in no way will be accountable for the handling of E-Mail by non-university providers. By redirecting their E-Mails, students, faculty or staff are not absolved from the responsibilities that exist with official communication sent to their @shreevidyauniversity.edu account.

Authentication for Confidential Information

If any user of official E-Mail address impersonates university's office, faculty/staff member or student, it is considered to be a violation of university policies, including the Student Code of Conduct. In order to reduce such risk, some confidential information may be made obtainable only through "My Connection" which is a secured connection allocated to student and is protected by password. In such cases, students will receive E-Mail communication directing them to "My Connection," where users can access the confidential information by supplying their university ID and PIN. The confidential information will not be obtainable in the E-Mail message.

Privacy Protection

Users should use utmost care while using E-Mail for communicating confidential or sensitive matters. Users should not take for granted that E-Mail is private and confidential. It is particularly vital that users should take care to send messages only to the intended recipient(s). Special care should be taken when using the "reply" command in E-Mail communication.

Educational and Administrative Uses of E-Mail

Faculty at Shree Vidya University will determine how they will use electronic forms of communication (e.g., E-blogs, online discussion boards, etc.) in their classroom sessions which will spell out their course syllabus requirements. The official E-Mail policy is to make sure that all students will adhere to E-Mail-based course requirements stated by the faculty. It can be assumed that students' official @shreevidyauniversity.edu accounts are accessible and faculty can use E-Mail for their classroom sessions accordingly. Administrative offices will determine the use of E-Mail communications for administrative purposes.

University Announcements

Appropriate authority, on behalf of Shree Vidya University, can provide approval for transmission of E-Mail containing essential university announcements to students, faculty and staff. Only the offices of Faculty Heads/Department Heads or the University Chancellors are authorized to do the broadcasting messages to a wide audience of students, faculty and staff. Mass mailing communications to external university audiences must be minimized. If mass mailing is done, it should be accomplished utilizing an appropriately identified third-party service to mitigate the placement of university.edu E-Mail servers on Spam blacklists.

Ownership/Administration

The university owns all E-Mail accounts run on its system. Under some conditions it may be essential for the ITS staff or other suitable university officials to access E-Mail files to keep the system up, and to look into security incidents or data abuse incidents or violations of other institutional policies. Such access will be on a need-to-know basis and any E-Mail accessed will be made known only to those persons who need to know or as required by law. Although incidental non-business personal use of E-Mail is good enough, conducting business for a commercial basis using university computer resources is prohibited. Share, highest message size, message preservation settings, expiry settings, continuance times and other E-Mail guidelines will be set as appropriate for the anticipated volume and platform scaling. The need for revised settings will be monitored with changes made as per appropriate recommendations (see E-Mail guidelines at http://www.shreevidyauniversity.edu/helpdesk/email).

Termination

Shree Vidya University provided E-Mail accounts to students, faculty and staff. These E-Mail accounts are treated as components of electronic services only when they are engaged with the university. Refer to Section III K of this policy (Termination of Access to University's Computing Facilities). In some cases, employee E-Mail accounts may be sustained for a longer period or forwarded for appropriate usage as deemed fit by the university.

Violations/Abuses

Breach or mistreatment of the policy may result in limited access to university's E-Mail system. In addition, this may also call for other appropriate disciplinary action as deemed fit by the university.

C. LISTING Service

Establishing the LISTING Service

List content must practically demonstrate the tasks, field of know-how, research or study of the list sponsor with regard to his/her function at the university. Sponsors and owners of list are expected to adhere to all computing resource usage policies put forth by the university.

Sponsorship/Ownership of the List

1. Only faculty/staff, which is on permanent role of the university, may sponsor a list.
2. Owners of the list have the responsibility for adequately conveying to the list membership – this would usually be in the form of an agreement/welcome message sent to all new subscribers to understand the guidelines for list posting. Owners should also make sure that their subscribers are in the know of the required list configuration settings that are vital (e.g., who can post, who can subscribe, etc.).
3. List owners should take the responsibility for ensuring that at all times there exists an appropriate membership, as related to university functions.
4. List owners are in charge of updating the subscriber list and removing or suspending unacceptable or difficult addresses.
5. Institutional lists maintained for the purpose of announcements, news and professor talks will be maintained by the ITS LISTING Service Manager.

List Content and Copyright

1. List subscribers, owners and all others with list posting privileges should adhere to copyright restrictions applicable when loading any material not owned by them. Using a mailing list for distributing any material (including binary files) is strictly prohibited if it is in violation of copyright or licensing.

List Expiration and Renewal

1. With the only exception of class lists, all other lists expire annually at the end of each semester (within a week of ending the final exams). Class lists terminate at the end of each semester (the week after the end of final exams). Lists less than 3 months old, at the time of termination, will not expire until the end of next semester or academic year, whichever is applicable.
2. All list owners will be notified by E-Mail at least 3–4 weeks prior to the expiration date. For renewing a list, the list owner must respond to the renewal announcement stating the purpose to bring up the list again.
3. In the event if the list owner does not respond even after two termination notices and does not confirm that he/she wants to renew the list, then the list will be deleted.

List Removal and Deletion

1. A list may be deleted at any time by the LISTING Service Manager at the request of the list sponsor.
2. ITS is authorized to delete lists that:
   - are misused.
   - do not adhere with recognized policy.
   - pose a danger to system security or integrity.

In such cases, the LISTING Service Manager will try to inform the list sponsor and/or primary owner prior to the deletion of the list.

Information Technology Services' Rights

1. Shree Vidya University's ITS provides LISTING Service as a service to the community associated with this university. By itself, ITS keeps the authority for making changes in the service at any time for the sake of the common good of all users.
2. The LISTING Service Manager reserves the right to make changes to any list's configuration without notice in the following cases (not exhaustive):
   - To correct errors.
   - To make preferred changes or improvements.
   - Where the list owner has been negligent or lax in conducting required list maintenance.
3. The LISTING Service Manager reserves the right to restrict or deny any user access to or privileges on LISTING Service with due cause. The LISTING Service software may automatically and selectively deny service to users based on bounced or excessive E-Mail or other detected problems.

D. The University Website

The University Website and Use of the Web Servers

1. The university website, which begins at the homepage www.shreevidyauniversity.edu, is a volume of documents on several servers created by diverse authors which, as linked, represents the university as an official publication.
2. All departmental or student group web pages are part of the official university website, and are screened, monitored, coordinated, supervised and controlled by the university webmaster, who retains the right to edit the pages.
3. All authorized university web pages must be designed based on standards of technology or content specified by the university webmaster or any superseding authority on the matter of website design appointed by the university.
4. Authorized users of the web servers (for official or individual pages) shall be no more than 8 MB of hard drive space per folder. All space is to be devoted to webpage use only. The university may allow authorized individuals more than 8 MB of space if a genuine academic need is described to the webmaster. No personal file storage or other file activity is permitted on the web servers.
5. When notified that they are exceeding the 8 MB limit, authorized users must delete a necessary amount of material in a time period specified by the webmaster or risk deletion of all files.
6. Except that access is gained by request, web server and website user responsibilities and access policies are the same as those under Sections III, IV and VI of this document.
7. All personal and official web pages will be free of content articulated in Sections I and II of this document in addition to pornography, hate speech and non-university sponsored E-Commerce.
8. Any official or personal web pages that use technological features beyond HTML, Java, JavaScript, client-side VBScript must be taken through review by and approval from the webmaster appointed by the university.
9. Web pages using applications such as active server pages (ASP) must be submitted for review and approval by the university webmaster.
10. Universal write access is forbidden on any private or official page.
11. When a violation of these policies occurs, university reserves the right to remove any and all contents in any files or folders on the web server without advance notice or consultation, and to revoke server permissions to any authorized user.
12. Instances of violations discovered by the webmaster may be notified to appropriate university authorities.

University-based groups of all types (including student groups) who choose outside web developers shall take the responsibility to oversee and maintain quality control measures in order to meet the standards of technology and content set by the university webmaster or any superseding authority appointed by the university. Outside developers, with no current, formal or direct affiliation with the university shall not be allowed to possess personal accounts on the web servers that belong to the university. All student groups and/or departments or those who decide to have an outside developer work on their web pages must contact the Help Desk before commencing work.

All web pages, images or files located on the university web servers must be maintained and updated to reflect current and accurate content. In no instance should the web servers be utilized for storage or archiving purposes. Files that are no longer active or current must be removed from the university web servers periodically upon the request of the university webmaster or risk removal as deemed appropriate by the webmaster. The webmaster will once in a while send reminder to campus community to purge its web server directories of all inappropriate or out-of-date files.

Web publishers are accountable for the content of the pages published by them on the university web server. They are also expected to abide by the highest standards of quality and responsibility. Content must be relevant to the university. Web authors and publishers are required to comply with all university policies, as well as all local, state and federal laws concerning appropriate use of computers and the Internet. Departmental web pages must follow the design standards laid down by the university. Refer to guidelines for developing and publishing new web pages located at: http://www.shreevidyauniversity/webdesign/guidelines.asp

The reason for providing the webpage is to present information to students and colleagues. The webpage, at a minimum, must contain the following:

1. All TITLE tags placed within HTML files must use the following format to promote uniformity, clear page recognition and boost rankings in search engines:

TITLE FORMAT: Page Title – Departmental Name, University Name
Example: <TITLE>Electronic Journals, Dabke Anil. Ramakrishna Library,
University
University</TITLE>

2. All web pages must include the university name "University." The rationale is that this will help identify the location if the user has entered the website without going through the homepage.

3. All pages must include a link back to the university homepage (http://www.shreevidyauniversity.edu).

File names should NOT include spaces, hyphens (-), underscores (_), alpha and numbers 0–9 are permissible.

Correct Example: FileName.html
Incorrect Examples: File Name.html, File-Name.html, File_Name.html

All web pages must adhere to requirements for minimum web accessibility set forth by the association of disabled individuals and mandated by the ensuing policy. This policy requires that all websites of state's agencies provide universal accessibility to persons with disabilities.

Shree Vidya University will sponsor and host websites for non-university, non-profit organizations provided that their purpose is relevant to the mission of Shree Vidya University, and only if there is a dynamic member of the university campus community (faculty or staff in a current appointment) who is ready to be the *sponsor* for that website. A special group account will be issued to *sponsors* and that account can be used by the web developer. The *sponsors* will have the responsibility to maintain and monitor the organization's web pages. Before uploading to the Shree Vidya University servers, the sponsor must submit all new websites or web pages for review and approval by university's webmaster. *Sponsors* must also inform Shree Vidya University's webmaster when the content on any of the pages is modified. These non-campus-hosted websites must abide by the policies that are specified for official university web pages. The university webmaster is authorized to edit content and annul server permissions to any authorized user who does not work in congruence with the policies set forth by Shree Vidya University.

Personal Web Pages

Users may create their own homepages. File Transfer Protocol (FTP) access to a personal directory on the university server will be provided to the university's faculty and students, so that they can maintain their own homepage files. Under no conditions personal space and/or files are allowed to be shared with other users. While making a design for a personal homepage, it must be remembered that use of homepages for personal profit is strictly prohibited. Additionally, it is to be remembered that the design of personal homepage must not violate copyright, pornography or any other prevailing laws. Shree Vidya University has the exclusive right to monitor all work on the server and may remove any personal homepage or files if it is found that they have violated any of the policies. In addition, failure to abide by computing policies could, in some cases, lead to disciplinary action or criminal prosecution.

Blog and Forum Standards on University's Website

University website services provide server space, forum and web log or blog services in support of scholarly, academic, extra-curricular and professional communications conducted by members of the university community who have network accounts. Standards for posting behavior are as follows:

1. The material posted on the website should be free of offensive, racist, sexist and homophobic text. It should not be framed in a manner that may sound offensive. There should be no personal criticism against identifiable individuals.
2. Website postings should be consistent with the topic and should be true to the theme or use of the blog or forum.
3. The statements "*The views and opinions articulated on this page are absolutely those of the page author(s)*" and "*The contents of this page have not been reviewed or approved by the university"* must appear on all blog and forum pages that may be sponsored by Shree Vidya University.
4. The university makes it mandatory to use university-approved templates for blog and forum administrators on all hosted pages.
5. In case the contents of blog and forum are found to violate Shree Vidya University's website policy or any prevailing law, the university will have the right to get rid of such content or the blog or forum module itself. The university also has the right to do the same at its sole discretion when it is deemed appropriate to do so.

Supplementary Web Design Standards for Official University Websites

Besides accessibility requirements mentioned above, all official university websites must also meet the layout standards mentioned below because those standards are proposed to maintain site-wide navigation and design consistency.

1. All official university websites must use an approved web design template.
   Visit the link at: http://www.shreevidyauniversity.edu/templates/global_files.zip (800 KB). A sample template site is available at:
   http://www.shreevidyauniversity.edu/templates/global_files/sample_site/%20
2. It is required that at the top of all official web pages of Shree Vidya University, the overall top navigation bar must appear. The source code for the global top navigation bar is available at: http://www.shreevidyauniversity.edu/templates/global_files/topnavbar/topnavbar_inc.asp
3. The global top navigation bar also requires an accompanying design file: http://www.shreevidyauniversity.edu/templates/global_files/topnavbar/topnavbar.css

Requests for Exemptions

Academic or administrative departments who would like to seek exemptions to the above design and navigation standards for official websites of Shree Vidya University can mail or E-Mail their request to: Chairperson, Web Steering Committee c/o Webmaster, University Avenue, 252 Central Road., Pune, 4110016, Maharashtra, Tel.020-67343323. The Web Steering Committee will review the request and forward its recommendations to ITAB for review and consideration. At minimum, the global top navigation bar is required for all official university pages, unless technical issues prevent its inclusion.

E. Learning Management System (LMS)

1. The policy for learning management system will address items not already covered by another policy or regulation (as the case may be).
2. Access defaults should reflect Banner data ease of access rules.
3. Faculty can see profile data (address and phone number) for students in their classes.
4. Students can see profile data for faculty.
5. For authenticated users, directory information will be available.
6. Shree Vidya University protects students' privacy rights. Therefore, students who wish to have discretion of directory information via the Registrar will be granted confidentiality in LMS and indicated as confidential to faculty.
7. Banner data determines LMS course enrollments with a nightly add/drop. Accounts and Roster entries are added nightly. Drops and withdrawals are marked as "disabled" in the LMS course roster. There will be no self-enrollment for students in courses. Faculty may allow access to others at their discretion. When courses are ready to deliver, they can be searched and accessed by students.
8. Undergraduate students are not authorized to access the LMS course result book. This item is currently under review and will be audited until a final decision is made.
9. Students will be allowed the role of Group Leader and will be able to request a group be made for online collaboration from any university employee who agrees to sponsor their online group. Student Group Leaders can add members to the group if they know the Fredonia E-Mail address of the potential member. They will not be able to list LMS accounts or educational records. They will only see directory information.
10. Librarians will have access to courses for those who request reserve materials. Reserve readings will be published to LMS courses regardless of whether the instructor uses LMS for the class. Permission is granted to library staff by the instructor via the reserve request form.
11. Campus members may submit public items (news, events, forums, polls and surveys) to the LMS Administrator to post in public areas of LMS. Items will be selected based on their academic nature and relevance to a general student audience. Policy is under developed to promote increased access to public components.
12. University ID photos will be added to LMS to allow instructors to view photos of students enrolled in their classes. (Target: <ddmmyy>.)
13. Campus members may request guest LMS accounts by E-Mailing the LMS Administrator. This item is being reviewed by the Electronic Services Group.
14. At this time, there are no plans to delete LMS accounts. When students complete their academic program at Shree Vidya University, their accounts will be disengaged and access rights will be revoked and their status will be changed to "ALUMNI." Alumni accounts may be activated as part of the portfolio implementation. Staff who leave and students who do not return will also be disabled and categorized as "external." Enrollment process all over again may be required in such cases.
15. Using the Banner data, groups will be automatically created for use by Departments and Advisors. (Target: <ddmmyy>.)
16. Data purge policies are under development to ensure data privacy protection.

F. Virtual Private Network (VPN)

Shree Vidya University's ITS department provides a Virtual Private Network (VPN) mainly for ITS staff to remotely and securely monitor and administer systems as necessary. The principles, mentioned below, are intended to reduce the likely exposure to the university from damages, which may result from illegal use of university resources. Damages include the loss of sensitive information or University's classified data, intellectual property, harm to public image, damage to university's vital internal systems, etc. VPN use on a limited basis is provided for employee administrative access to "not to be disclosed" databases when distant work-related business is absolutely necessary, and when the employee has been provided with a need-based level of access appropriate for his/her usage along with approval for such access. Individuals, who are provided with VPN privileges, must appreciate and agree to the following:

1. They are responsible for selection, coordination and installation of high-speed connectivity through an Internet Service Provider (ISP).
2. They are responsible to see to it that only authorized users are allowed access to university's internal networks via their VPN.
3. VPN use is controlled using password authentication.
4. VPN gateways will be set up and managed by university's ITS, and only ITS-approved VPN clients may be used.
5. Users appreciate that by using the VPN technology with their personal computers, their computers, in effect, become an extension of Shree Vidya University's network. Per se users become governed by the same rules and regulations that apply to university-owned computing equipment, that is, their personal computers (connected to university network) must also be configured to abide by Shree Vidya University's security policies, which also include the latest operating system security patches and antivirus software definitions.
6. ITS can provide desktop support and connectivity issues related to VPN access only for university-owned equipment.

VI. Unauthorized Use

Shree Vidya University considers it unethical whenever there is an infringement of the regulations mentioned above. Such violations may constitute a criminal felony. Offenses will be handled with cognizance to any or all of the following: applicable laws, country's Penal Code; the Shree Vidya University announcement on "Student Rights and Responsibilities"; other applicable laws prevailing, regulations and policies of the campus. Offenses may result in the deferment or permanent closing of usernames, actions as per rules for campus disciplinary procedure, legal action and/or other action.

When ITS or the RemoteNet Office becomes aware of a possible violation, the university will initiate an investigation in conjunction with the campus Security Administrator and/or relevant campus offices including the Office of Student Affairs, Human Resources Office and the Police stationed on the university campus. Upon being requested, users are supposed to collaborate fully in such investigations.

For preventing further illegal activity during the course of such an investigation, ITS may delay authorization for use of all computing facilities for the user(s) involved in the violation. Remote Access administration team reserves the right to temporarily suspend a user's Internet connection pending the outcome of any required Administrative Sanction Hearing. The categories of unauthorized use, mentioned below, are only a few examples – the list is not exhaustive.

A. Academic Dishonesty

Shree Vidya University prohibits any form of dishonest practices through use of computing facilities (e.g., cheating in day-to-day circumstances/cheating during the exams, plagiarism in assignment and project work or fraud/dishonest behavior).

B. Harassment

Use of computer(s) or computer networks to pester, mistreat or threaten another individual is forbidden. Users shall not develop or use programs that annoy other users. Users shall show responsive behavior when availing publically shared facilities (e.g., gardens and cafeterias/canteen establishments on campus, etc.). Users should take care not to exhibit in such locations images, sounds or messages that could create an ambience of uneasiness or annoyance for others.

C. Obscenity

Obscene/profane language in E-Mail, messages, process names, file names, file data and other publicly visible forms is prohibited.

D. Child Pornography

Law(s) pertaining to child pornography makes it illegal to create, possess or distribute graphic depiction of minors engaged in sexual activity, including computer graphics. Computers containing such information can be taken in custody for evidence collection activity.

E. Pornography

Shree Vidya University prohibits sending E-Mails with pornographic contents, file data, websites and other publicly visible forms.

Revised policy approved by authority of the University Dean <ddmmyy>

Further Reading

Additional Useful Web References

1. To understand parity bit and parity checking, refer to:
   http://www.webopedia.com/TERM/P/parity_checking.html (27 January 2011).
   http://en.wikipedia.org/wiki/Parity_bit (27 January 2011).
   http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci212748,00.html (27 January 2011).
   http://www.wisegeek.com/what-is-a-parity-bit.htm (27 January 2011).
   http://forum.allaboutcircuits.com/showthread.php?t=1710 (27 January 2011).