Dr. Harisingh Gour Vishwavidyalaya, Sagar.

Cyber Security Policy

(Release: Sep 2023 Version 1.0)

Table of Contents

I. Introduction

Information and Communication Technology (ICT) enabled technology can transform Governance by adopting best IT practices in Dr. Harisingh Gour Central University (DHSGSU). Dr. Harisingh Gour University offers various IT services for the various Academic/ Non-Academic process like Admission, Examination, Finance, Establishment, E-Content Services etc. to all the stakeholder of the University. The facility of MHRD-Wi-Fi is being provided in the University Campus for easy access of the IT-Services provided by the University.

These Cyber Security policies are carefully formulated to reduce risks to electronic information resources through implementation of controls designed to detect and prevent errors or irregularities that may occur. DHSGSU recognizes that absolute security of IT resources against all threats is an unrealistic preposition that would require the commitment of a prohibitively high level of resources. The Institution's goals for risk reduction are based, therefore, on the following principles:

- The criticality of an IT Resource to the operation of the DHSGSU.
- The sensitivity of the data residing in or accessible through the IT Resources.
- The cost of preventive measures and controls designed to detect incidents.
- The amount of risk that management at the campus or the Office of the Director is willing to absorb.

Achieving a successful information security program requires management/executive committee's planning for preparedness, detection, response and recovery with respect to protection of the information enterprise. Risk assessment and determination of appropriate security measures must be a part of all systems design and operations undertaken in the institution.

These Policies identify the set of measures that should comprise campus security programs. Security programs should include identification of the CISO (Cyber Information Security Officer) and DCISO who is responsible for campus compliance with its security program. Security programs shall undergo periodic evaluation of administrative, technical, and physical safeguards to ensure that they adequately address operational or environmental changes.

II. Appointment of CISO and DCISO

As per the guideline of Ministry of Education and Department of Higher Education, the university appointed CISO and DCISO as following:

Cyber Information Security Officer (CISO)	Dr. Rupendra J. Chourasiya Senior System Analyst & I/c Officer, IT Cell	No/R/2022/7/138, Dtd-14 Oct 2022
Deputy Cyber Information Security Officer	Sh. Sachin Singh Goutam Networking Administrator, IT-Cell	No/R/Estt./2023/8325, Dtd– 07 Jul 2023

III. Scope

These Policies apply to all students & Staff and to all entities/affiliates of DHSGSU. These Policies do not apply to the Research network and other affiliate laboratories. Implementation of these Guidelines, including development of more specific standards or guidelines as needed, is the local responsibility of respective stake holders and the Registrar. The Registrar of the DHSGSU has overall responsibility for implementing the policy, including these Guidelines on IT Security.

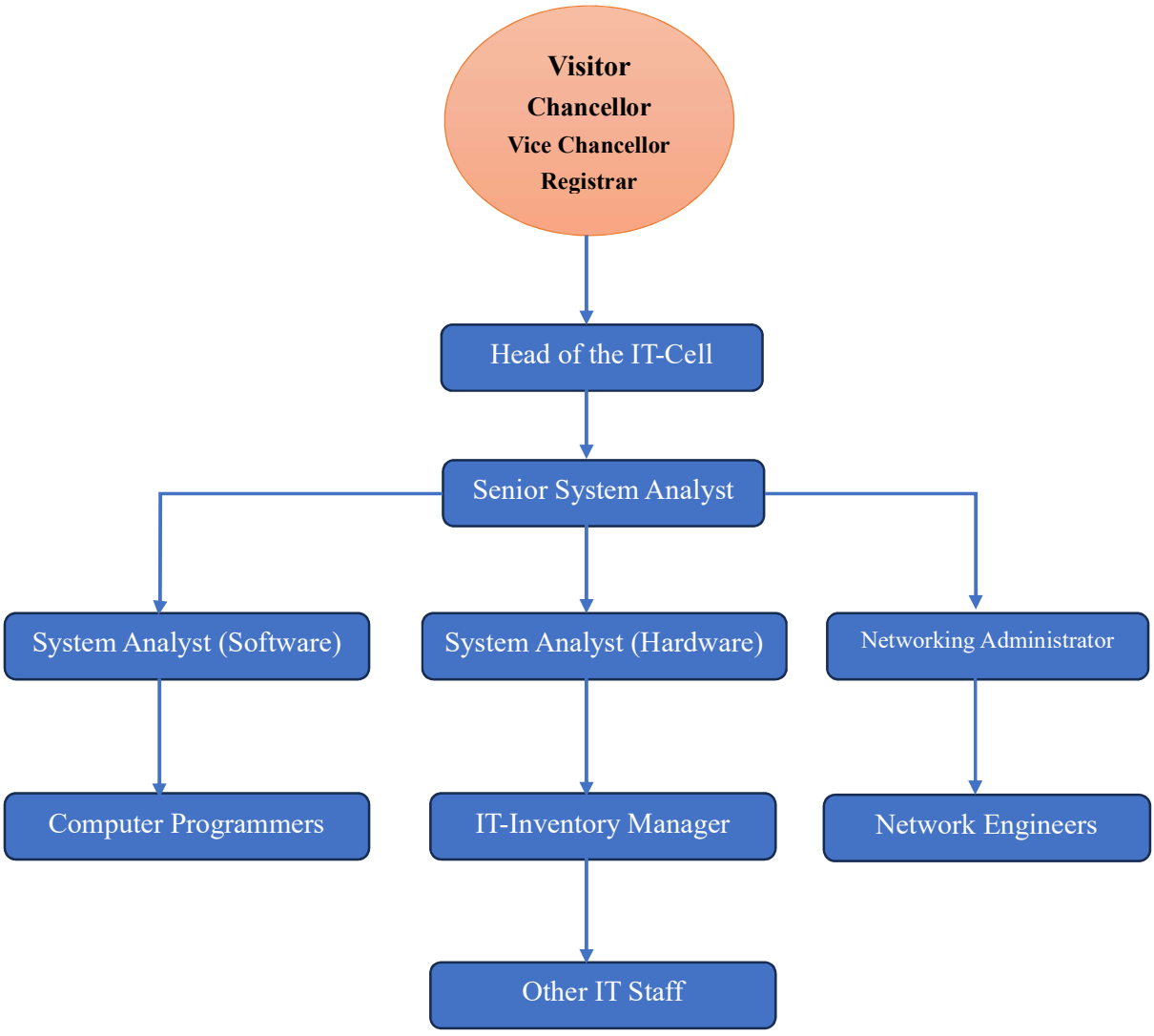
The DHSGSU Information Security Policy & Practices will be reviewed and evaluated once in a year for updates. Updates may include the creation of new Practices, modifications to existing Practices, and/or the deletion of line-item details. Updates can be triggered by several events including but not limited to:

- New technology including applications, hardware, or software
- Security deficiencies
- Changes in legal, regulatory, or reporting requirements
- Physical or environmental alterations
- Request for deviation from a Service Provider
- Periodic re-evaluation of current requirements

As DHSGSU esteemed central university of India, it is essential that all staff & students understand the value of DHSGSU's Information and their individual and collective responsibility to protect it.

IV. Organizational Chart

The security organizational structure is as shown below:



V. Responsibility

The various roles and responsibilities for DHSGSU personnel are defined as follows:

Registrar

Act as the custodian of IT security at DHSGSU. Functional Responsibilities

- Be the last word in any decision pertaining to the IT security of the Institute.
- Uphold the dictum of IT security ethics outlined in the policy
- Call for IT security reviews every month with CISO, Chairman computing.

Head of the IT-Cell

Act as the secondary in charge of the IT-Cell and the functionalities are as below:

- Be part of any decision pertaining to the IT security of the Institute
- Drive the user awareness sessions along with the CISO and DCISO.

Senior System Analyst

Act as Information IT, IS and Security Manager for the organization. Functional Responsibilities

- Act as Cyber Information Security Officer.
- Be the Institute's single point contact on information security.
- Promote information Technology and security awareness for all the Staff & Students in the institute.
- Develop, implement, revise and document location-wide (and subsequently institute wide) security policies.
- Periodically review the status of the information Technology infrastructure and security policy implementation in DHSGSU and report the status to the office of the director
- Be part of the decision-making team when the organization is involved in designing, planning, procuring or upgrading technologies.
- Conduct formal / informal training on relevant topics on security like firewall implementation, VPN configuration within the IT staff.
- Act as the single point of contact for all issues involving information security including, but not limited to, questions, alerts, viruses and breaches.

System Analyst (Hardware)

- Plan, implement, monitor, administer and upgrade security controls for DHSGSU's computing infrastructure and environment (Computers and VM's in datacentre).
- Help develop internal security standards for DHSGSU in consultation with IT & IS Manager. Functional Responsibilities
- Test, install, and maintain security infrastructure equipment.
- Help define, document, and maintain DHSGSU security policy.
- Monitor, audit, test the systems and networks for possible security threats and vulnerabilities.
- Review security log files on a daily basis, investigate and report anomalies and breaches.
- Be abreast with the technology changes and continuously evaluate possible threats resulting from technology changes to the organization's existing computing and network infrastructure.
- Investigate, coordinate, report, and follow-up on computer network security incidents.
- Disseminate DHSGSU security policy and procedures to the appropriate entities on a need-to-know basis.

System Analyst (Software)

- Perform regular security audits and take corrective action as required. These audits may cover attempts to crack user passwords; maintenance of system logs of network activity in order to watch for attacks on network/system security; deletion or alteration of system- related files in user accounts; deletion of files or processes that are jeopardizing the security of a user account or of the system as a whole or which have resulted in degradation of system performance.
- Perform periodic backups of user and operating system files. The frequency of these backups will vary from system to system. Periodically reorganize file systems while ensuring that proper file security is maintained.
- Inspect, edit or delete private information (whether in the form of user accounts, files, processes, etc.) as required, and dealing with incidents of suspected inappropriate use".
- Apply patches and upgrades to operating systems and utilities as available.
- Inform the users of the system about planned outage/unavailability of the system so that they can plan their work accordingly.
- Monitor console message during shifts and ensure data protection, diagnose and recover system failures. Maintain production/uptime/hardware fault logs.
- Ensure data security by taking regular/off site/Monthly backups, in accordance with specified schedule/contingency plans as decided from time to time.

- Trouble shooting of any hardware-related problems on PC's and also inform IT-Cell about the status of the call.
- Fault isolation, installation and diagnosis of Server/PC hardware.
- Co-ordinate with Vendors for corrective maintenance of all hardware peripherals as and when required.
- Ensure the maximum uptime of links, Internet and maintain the logs of uptime/downtime of this hardware. .
- Allocation/tracking of laptops and maintain the necessary logs.

Network Administrator

- Act as Deputy Cyber Security Officer of the University.
- Install, maintain, administer, support and upgrade the networks (LAN/WAN) in DHSGSU. Support and administration of DHSGSU computing and LAN networking.
- Functional Responsibilities
- Configure workstations and servers on Microsoft Windows / Linux platforms for the networks.
- Install network monitoring/administration tools and troubleshoot the problems with the networks.
- Ensure uptime of networks and support the links for all the building blocks of campus.
- Support helpdesk personnel for server and network related issues.
- Perform off-line server activities such as backups.
- Configure LAN and WAN switches, Access Points, hubs, and routers.
- Install and ensure security controls such as firewalls and proxy servers are functioning properly.
- Evaluate network-monitoring tools and recommend relevant tools that will enhance the network and provide defined security.
- Report any breach of security on the servers that are assigned for monitoring

IT-Cell Personnel (IT support /Helpdesk outsource work force)

- Perform IT-Cell's activities as outlined in the contract for the activities.
- Functional Responsibilities
- Receive, assign and record support calls from users. Ensure that the problems are resolved within the stipulated time period.
- Reassign/escalate the calls based on the nature and status of the calls.
- Execute helpdesk activities and collect feedback through various mechanisms especially for day-to-day desktop support calls

- Provide suggestions on improving service levels based on the day-to-day experience and the feedback and data.
- Take initiative in implementing directives resulting out of change in processes related to desktop management and other support activities in a timely manner.
- Implement and support the solutions based on the problem reported and follow change management processes as defined in change management.
- Plan and caution the users well in advance about problems anticipated and changes that are planned before they are affected.

VI. Backup & Recovery Policy

Backup and Recovery

- Back-up copies of essential academic data and software shall be taken regularly by System administrator and shall reflect the needs of the academic/research and also any legal and regulatory requirements. In his absence, other personnel designated by the data center administrator shall take backup.
- Adequate back-up facilities shall be provided to ensure that all essential academic/research data and software could be recovered following a computer disaster or media failure.
- A formal documented backup plan and schedule shall be authorized by the IT and IS Manager and shall be implemented and followed by the System administrator.
- The criticality, backup and frequency of backup of the information with respect to the applications managed by the DHSGSU network shall follow the Backup plan. A monthly review of the Backup plan shall also be conducted.
- The IT and IS Manager shall formally intimate the System administrator about any new applications and its data to be backed up. Similarly, the System administrator shall be informed about discontinuing the backup of the applications systems no longer in use at DHSGSU.
- Desktop, laptop and hand held computers are not backed up by the system administrator.
- DHSGSU Staff and students who use laptops or hand-held computers shall ensure that these are regularly backed up using external media such as floppy disks, CDs, Pen Drive, Portable Hard Drive etc.
- System Administrator shall be responsible for full back up, archiving and restoration of all servers as nominated and listed as Core systems by the IT & IS Manager. The network provided Home directories shall be backed up each night for "differential changes" and a full system back up once per week. This shall include at a minimum:
    a) Servers
    b) Databases

- System/Networking Administrator shall be responsible for full backup, archiving, and restoration of all the router configuration files and firewall rule bases.

Backup Controls

- At least three generations of back-up data shall be retained for important applications. System administrator shall establish and formally document an appropriate schedule of full and incremental backups.
- A minimum level of back-up information, together with accurate and complete records of the back-up copies, shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site.
- Back-up data shall be given a level of physical and environmental protection, consistent with the standards applied at the main site. The controls applied to media at the main site shall be extended to cover the back-up site.
- Backup data shall be regularly checked, to ensure that they could be relied upon in an emergency.
- Data shall be retained for the period necessary to satisfy both business and legislative requirements. Data owners shall identify the retention period for essential academic data, and shall establish any requirement for archive copies to be retained.

Backup Media and Security

- The storage media used for the archiving of information must be appropriate to its expected longevity.
- The format in which the data is stored must be carefully considered, especially where proprietary formats are involved.
- It shall be ensured by System administrator that the media is regularly examined as per the media vendor recommendations. The backup media shall also be replaced as per the vendor recommendation on number of rewrites.
- The backup media shall be appropriately labelled and numbered.
- Backup media shall be controlled and physically protected. Appropriate operating procedures shall be established to protect tapes, disks, data cassettes, input/output data and system documentation from damage, theft, unauthorized access and virus attacks as appropriate.
- There shall be clearly documented procedures for the management of removable computer media, such as tapes, disks, cassettes and printed reports.
- Media containing unclassified but sensitive material shall be distributed through normal channels. Media containing unencrypted, classified information shall be delivered through approved safe hand channels only. A formal record of the authorized recipients

of media containing classified information shall be kept and receipt notification requested.

- Media shall not be removed from the department without written authorization. An audit record of all such removals shall be maintained.
- All media shall be stored in a safe, secure environment, and in accordance with the manufacturers' specifications.
- Media no longer required and planned for release or disposal from the department shall be purged in an approved manner before release. Media holding up to and including CONFIDENTIAL information shall be overwritten with an approved utility; media having held higher-grade information shall be destroyed.

Storage of backup

- On-site data backup shall be maintained in safe custody, preferably outside the server room and in a fireproof cabinet. The key to the cabinet shall be available only with the System Administrator and the duplicate shall be kept with IT & IS Manager for emergency use.
- Off-site data backup shall be maintained at a location identified as 'off-site' by the IT & IS Manager. Every two weeks, the backup media is moved to and from off-site location, it shall be carried in sealed and tamper-proof envelope or pouch.

Backup logs

- The backup logs maintained by the Systems Administrator should either be manual registers or the reports generated by the system, which should be printed, and hard copies maintained.
- Systems Administrator should also maintain the backup movement logs for the backups at off-site location. Backup Restoration
- The user should make an application to their Department Head (stating the reasons for restoration) for approval of restoration of data. . Department Head should ensure that the user has the right to access the data required for restoration prior to granting the approval.
- Upon receiving the authorization, the data should be restored by the Systems Administrator.
- A log has to be maintained by the Systems Administrator which should contain date and time along with name and signature of the person who required / requested for the restored data. Log should also include number of backup media used for restoration.
- All the backup media, which were used for restoration, should be returned to the offsite location after the restoration is complete in a sealed and tamper proof envelope.

Restoration testing

- To verify the readability of backup media, mock restoration tests should be carried out at least once in 2 months on the Testing server.
- The entire process should be documented detailing the test plan, the procedures executed and the test results.
- All the backup media, which were used for restoration, should be returned to the offsite location after the restoration is complete in a sealed and tamper proof envelope.
- It should be ensured that the restored data is deleted after successful completion of testing.

VII. Password Policy

Policy Statement

The Policy states that, the information assets of DHSGSU would not be compromised because of weak passwords in systems and infrastructure devices which host it.

To provide a mechanism to maximize the security of information stored on DHSGSU's IT infrastructure through the appropriate use of passwords.

Passwords are assigned to each individual as a method to control and monitor their unique access to systems and information, and should never be shared with others.

As a policy – all logon IDs in DHSGSU's domain should have password as per the following details

- Length of password: The password should be of minimum eight alphanumeric characters. Password selected should be case sensitive.
- Characters in Password: Should contain both upper and lower case characters (e.g., a-z, A-Z)
- Content of password: Should have digits and punctuation characters as well as letters e.g., 0-9, @#$%^&*()_+|~- =\`{}[]:";'<>?,./)
- Password History: Previous five passwords cannot be repeated. This means users cannot use the last five passwords.
- Maximum Password Age: Password expires after 90 days after it was last changed. However it gives a warning message after 70 days. However users can change the password at there wish before 90 days as well.
- Minimum Password Age: Once the user changes the password, he/she should not be able to change the password within 1 day.
- Account Lockout: Account will get locked after 3 Invalid logon attempts. This is to prevent any other user trying for your password for long.

- Passwords shall not be displayed in any environment (including on office walls, desks and workstations) at any time, including during sign-on procedures.
- Compromised passwords, or those suspected of being compromised, shall be immediately changed.
- Passwords stored in computer files and/or documentation shall be encrypted.
  Password reset will be done by IT Team on request, if user forgot the password or user does not remember the password.
- User is responsible for all actions and functions performed by his/her account.

Strong Password Characteristics:

Passwords are used for various purposes at DHSGSU. Some of the more common uses include; user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Everyone should be aware of how to select strong passwords.

- Are not a word in any language, slang, dialect, jargon, etc
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. **NOTE**: Do not use either of these examples as passwords!
- Do not use the same password for DHSGSU's accounts as for other non-DHSGSU access (e.g., personal ISP account, Internet mail services, net-Banking etc.). Where possible, don't use the same password for various DHSGSU access needs. For example, select one password for the Personal use and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.
- Do not share DHSGSU passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential DHSGSU information.

General Password Construction Guidelines:

- All system-level passwords (e.g., root, enable, Domain Admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 60 days.
- Passwords must not be inserted into email messages or other forms of electronic communication
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the

passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

- All user-level and system-level passwords must conform to the guidelines described above

Here is a list of "don'ts":

- ☒ Don't reveal a password over the phone to ANYONE
- ☒ Should not be a word found in a dictionary (English or foreign)
- ☒ Should not be a common usage word such as
- ☒ Names of family, pets, friends, co-workers, fantasy characters, etc.
- ☒ Computer terms and names, commands, sites, companies, hardware, software.
- ☒ The words "DHSGSU", "Dr. Harisingh Gour Vishwavidyalaya, Sagar"," Welcome" or any derivation
- ☒ Birthdays and other personal information such as addresses and phone numbers.
- ☒ Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- ☒ Any of the above spelled backwards.
- ☒ Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- ☒ Don't reveal a password in an email message
- ☒ Don't talk about a password in front of others
- ☒ Don't hint at the format of a password (e.g., "my family name") □ Don't reveal a password on questionnaires or any forum.
- ☒ Don't reveal a password to the boss
- ☒ Don't share a password with family members
- ☒ Don't reveal a password to co-workers while on vacation
- ☒ Do not use the "Remember Password" feature of applications (e.g., IE, Crome, Firefox, Outlook, Etc…).
- ☒ Again, do not write passwords down and store them anywhere in your work area. Do not store passwords in a file on ANY computer system (including Palm top or similar devices) without encryption.

"Do's"

- ☑ Change passwords frequently as per the policy.
- ☑ If an account or password is suspected to have been compromised, report the incident to Helpdesk/IT-Cell and change all passwords.

DHSGSU, IT-Cell may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

VIII. Internet & Intranet Security Policy

Policy Statement

All information travelling over DHSGSU's computer networks that has not been specifically identified as the property of other parties will be treated as though it's an DHSGSU asset. It is the policy of DHSGSU to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

In addition, it is the policy to protect information belonging to third parties that has been entrusted to DHSGSU in confidence as well as in accordance with applicable contracts and industry standards.

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of the Internet.
- To educate individuals who may use the Internet, the Intranet, or both with respect to their responsibilities associated with such use.
- Unless specifically stated otherwise, all statements and policies will apply to both the Intranet and the Internet.

The new resources, new services, and interconnectivity available via the Internet all introduce new opportunities and new risks. This policy describes DHSGSU's official policy regarding Internet security and addresses the risk aspect.

Internet Access Restrictions

- DHSGSU IT-Cell reserves the right to exclude from Internet access to those services that have no reasonable relationship to the functioning of DHSGSU.
- The Internet usage timings shall be strictly controlled.

Internet Rules of Behavior

Using DHSGSU Internet facilities or equipment to make abusive, unethical or "inappropriate" use of the Internet shall not be acceptable. Examples of inappropriate employee Internet use include, but are not limited to, the following:

- Conducting or participating in illegal activities like gambling

- Accessing or downloading pornographic material
- Solicitations for any purpose which are not expressly approved by institution management
- Revealing or publicizing proprietary or confidential information
- Representing personal opinions as those of the institution
- Making or posting indecent remarks
- "Flaming" (e.g. malicious written attacks directed at someone) or similar written attacks
- Uploading or downloading commercial software in violation of its copyright
- Uploading or mailing of company's confidential documents without the permission/authorization of the concerned parties.
- Downloading any software or electronic files without reasonable virus protection measures in place
- Intentionally interfering with the normal operation of any other organizations Internet gateway

Prohibitions on User Internet Activities

To prevent any appearance of inappropriate conduct on the Internet and to reduce risk exposures to the organization, users shall not:

- Enter into contractual agreements via the Internet; e.g. enter into binding contracts on behalf of the institution over the Internet
- Use the institution logos or the institution materials in any web page or Internet posting unless it has been approved, in advance, by the institution management
- Use software files, images, or other information downloaded from the Internet that has not been released for free public use
- Introduce material considered indecent, offensive, or is related to the production, use, storage, or transmission of sexually explicit or offensive items on the institution network or systems
- Attempt to gain illegal access to remote systems on the Internet
- Attempt to inappropriately telnet to or port scan remote systems on the Internet
- Use or possess Internet scanning or security vulnerability assessment tools
- Post material in violation of copyright law
- Establish Internet or other external network connections that could allow other organisation users to gain access into DHSGSU's systems and information assets.

Authentication Required for Internet Access to DHSGSU's Systems

All users wishing to establish a trusted connection via the Internet with the DHSGSU's systems shall authenticate themselves at the existing authentication mechanism before gaining access to

the institution internal network. (Currently each device user provided MAC based Authentication by Aruba ClearPass)

All Internet/Intranet users are expected to be familiar with and comply with these policies. Any queries in this regard should be directed to the Head of IT. Violations of these policies can lead to revocation of system privileges and/or disciplinary action.

User Responsibility:

Users of DHSGSU's Network Internet connections must:

- Know and apply the appropriate DHSGSU Network policies and practices pertaining to Internet security.
- Not permit any unauthorized individual to obtain access to DHSGSU Network Internet connections.
- Not use or permit the use of any unauthorized device in connection with DHSGSU's Network personal computers.
- Not to use DHSGSU Network Internet resources (software/hardware or data) for other than authorized institution purposes.
- Maintain exclusive control over and use of his/her password, and protect it from inadvertent disclosure to others.
- Select a password that bears no obvious relation to the user, the user's organizational group, or the user's work project, and that is not easy to guess. Please refer to DHSGSU's Password Policy for details.
- Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.
- Report to the IT Manager or IT Support staff for any incident that appears to compromise the security of DHSGSU's Network information resources. These include missing data, virus infestations, and unexplained transactions.
- Access only the data and automated functions for which he/she is authorized in the course of normal business activity.
- Obtain course supervisor authorization for any uploading or downloading of information to or from DHSGSU Network multi-user information systems if this activity is outside the scope of normal learning activities.
- Make backups of all sensitive, critical, and valuable data files as often as is deemed necessary.

Enforcement

Violations of these policies can lead to revocation of system privileges and/or disciplinary action.

Information Movement

All software downloaded from non-DHSGSU Network sources via the Internet must be screened with virus detection software prior to being opened or run. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone (not connected to the network) non-production machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

It is also relatively easy to spoof another user on the Internet. Likewise, contacts made over the Internet should not be trusted with DHSGSU's information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal DHSGSU information.

Users must not place DHSGSU's material (software, internal memos, etc.) on any publicly accessible Internet computer that supports anonymous file transfer protocol (FTP) or similar services, unless the I/c IT-Cell or the respective stake holder has first approved the posting of these materials.

In more general terms, DHSGSU's internal information should not be placed in any location, on machines connected to DHSGSU's Networks, or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.

All publicly write able (common/public) directories on DHSGSU's Internet-connected computers will be reviewed and cleared periodically. This process is necessary to prevent the anonymous exchange of information inconsistent with DHSGSU's business.

Information Protection

Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, DHSGSU's secret, proprietary, or private information must not be sent over the Internet.

Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.

Credit card numbers, Debit card numbers, telephone calling card numbers, log in passwords, and other parameters that can be used to gain access to goods or services must not be sent over the Internet in readable form.

In keeping with the confidentiality agreements signed by all Faculty, Staff & Students, DHSGSU's research findings, software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-DHSGSU party.

Exchanges of software and/or data between DHSGSU and any third party should not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

DHSGSU strongly supports strict adherence to software vendors' license agreements. When at work, or when DHSGSU computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.

Likewise, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with DHSGSU's ethics, and are therefore prohibited. Similarly,

reproduction of words posted or otherwise available over the Internet must be done only with the permission of the author/owner.

Expectation of Privacy

Students & Staff using DHSGSU's information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties.

At any time and without prior notice, management/IT Staff reserves the right to examine email, personal file directories, and other information stored on computers. This examination assures compliance with internal policies, supports the performance of internal investigations.

Resource Usage

DHSGSU's Network encourages Students & Staff to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not on institution time. Likewise, games, news groups, and other non-business activities must be performed on personal, not on institution time.

Use of computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no business activity is pre-empted by the personal use. Extended use of these resources requires prior written approval of the respective stake holder.

Based on the usage pattern and status of Bandwidth, DHSGSU can implement web filtering of certain sites. Such list will be published to the Staff & Students and will be updated on regular basis.

Public Representations

Faculty, Students & Staff must not publicly disclose internal network information via the Internet that may adversely affect DHSGSU's credibility or public image unless the approval of the Office of the Director or Head of IT has first been obtained.

Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, and related public postings on the Internet. If Faculty, Students & Staff isn't careful they may let undesirable elements know that certain internal projects are underway. If a Student/Staff is working on an unannounced product, a research and development project, or related confidential matters, all related postings must be cleared by the one's Professor prior to being placed in a public spot on the Internet.

Reporting Security Problems

If sensitive DHSGSU's Network information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the IT Team must be notified immediately.

If any unauthorized use of DHSGSU's information systems has taken place, or is suspected of taking place, the IT team must likewise be notified immediately.

Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the IT team must be notified immediately.

Because it may indicate a computer virus infection or similar security problem, all unusual systems behaviour, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

IX. Antivirus Policy

The anti-virus policy is designed to deal with the known virus that DHSGSU IT team is aware of & also the zero-day vulnerabilities that may arise.

General Guidelines are:

Deployment and Configuration of anti-virus software

- All computers of DHSGSU including servers, desktops & laptops shall have standard and supported anti-virus software installed.

- The virus scanner shall be scheduled to run to scan for viruses at regular intervals. The scanning engines must be chosen to ensure defence in depth. Anti-virus controls must be placed such that any foreign content entering the organization is scanned by at least two different anti-virus technologies.
- A Centralized antivirus server shall be deployed to check all the incoming and outgoing traffic through Internet. The server shall be configured to verify against the virus signatures for both incoming and outgoing data/files of Email/message, ftp and http servers.
- Antivirus activities shall be centrally managed. Central monitoring and logging console shall be deployed, to monitor the status of pattern updates on all the computers and to log the activities performed on them.
- The IT& IS Manager shall identify a person or a team that is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free.

Maintenance/Updating of software

- Anti-virus software scanning engine and the virus signature files shall be kept up-to date. The time of updating the virus patterns shall be kept minimized. The time frame acceptable for updating the new pattern file shall be maximum 8 hours after the release of the patch.
- Periodic audit on all the users' desktops and laptops shall be performed to ensure that proper and latest version of virus engines and the definitions files are running and no virus threat exists. The user himself shall ensure that the XYZ approved Antivirus software is running on his working machine.
- All servers must have real-time and "batch" scanning enabled.

Containment and managing of virus incidents

- In the event of a virus outbreak, System-admin or IT Staff shall initiate appropriate action to contain virus infections and assist in their removal.
- Virus-infected computers shall be removed from the network as soon as they are identified, until they are verified as virus-free.
- Software downloaded from electronic bulletin boards, shareware, public domain software, the internet and other software from untrusted sources shall be prohibited unless prior authorization is received from the IT-Cell.
- A memory-resident virus protection program or a virus-scanning program shall be used on all files downloaded from diskettes, tapes, CD ROMs, or electronic connections.
- All hard disks serviced, or newly installed workstations (including portables) are scanned for viruses before use.

- Virus protection programs shall not be disabled.
- All virus detection incidents shall be logged, along with the action taken; Quarantine, Deletion or Successful cleaning.
- Logs shall be maintained on the Centralized antivirus server, and Alerts shall be configured to send warnings to the Incident Response Team and the originator of the email.
- All backups shall be checked for viruses during backup schedule. All restorations shall be checked for Viruses, before a restoration is made.
- When critical vulnerabilities are announced for application software, the patches shall be made quickly so that the window of exposure is very small. Application software shall include at a minimum, Windows7 or Windows10, Outlook, Internet Explorer, etc.

Awareness and training

- System Administrator shall maintain current knowledge and expertise on viruses and virus protection. This shall be kept up to date through suitable staff training, awareness and access to resources.
- CISO/I/c IT-Cell shall conduct a regular user awareness session for all staff on virus clean systems.

Responses to a virus infection

- Users must immediately call the Desktop Information Systems Help Desk/IT staff when they believe a system has been infected. The Incidence Response Team shall be then be contacted if required.
- The following information shall be provided if known: virus name, extent of infection, source of virus, and potential recipients of infected material.

The policy will cover the following areas:

- Desktop's
- Server's
- Email's
- Firewall's
- User awareness

For a detailed configuration and maintenance of the above-mentioned devices refer to the procedures.

Responsibility

DHSGSU IT Associates and users (faculty, Students & Staff) at individual location are responsible for the implementation and execution of this policy. IT & IS Manager is responsible for the monitoring of the successful implementation of policy. IT manager can initiate a revision in the policy.

Enforcement

Any Student/Staff found to have violated this policy may be subject to disciplinary action. The IT staff would is also empowered to take the affected system/device out of the network, without prior warnings what's so ever.

Procedures

The policy procedures will cover in detail the procedures to be implemented in the IT infrastructure of the DHSGSU to protect it against the virus threats.

The policy is designed to meet following types of viruses -

- ☑ Boot track and partition table virus
- ☑ Executable file virus
- ☑ Multipartite, parasitic, stealth and polymorphic virus
- ☑ Trojans and worms
- ☑ Malicious code and self-updating malicious code

Desktop Policy and Procedure:

This policy and procedures are applicable to all the desktops that are installed in the DHSGSU infrastructure. This is also applicable to all the partners or customers desktop/laptop that are connected to the DHSGSU infrastructure on a temporary basis.

Antivirus Software:

DHSGSU approved antivirus software has to be installed on all the desktops that are connected to DHSGSU infrastructure on a temporary or permanent basis. This is applicable to all the laptops which are disbursed among the students and staff.

Antivirus Signature

Antivirus signature must be updated on the entire desktop automatically when the antivirus signature is updated. In case of a virus outbreak the desktop should be forced to update the virus signature and IT team should ensure that the entire desktop in the DHSGSU infrastructure has an updated virus signature.

Desktop Antivirus Configuration

All the desktops/laptops in the DHSGSU infrastructure should be configured as per the following configuration –

- ☑ Enable system real time protection.
- ☑ Enable start-up scanning of memory, master/boot record, and system files.
- ☑ Enable scanning of all the files in your system.
- ☑ Logging should be enabled for all the desktop virus related activity.
- ☑ Schedule a scan of the desktop daily.
- ☑ All virus related security patches should be installed on all the desktops.
- ☑ Set site attribute of wsock32.dll to read only.
- ☑ Set the attribute of normal. dot to read only.
- ☑ Enable the floppy to be scanned before use by the desktop.
- ☑ Software will be installed only from approved internal server to limit exposure to contaminated software.

Server Antivirus Policy

Servers are the centralized resource for all the staff & students and it should be adequately protected since it can become the probable cause of widespread of virus.

Following procedures have to be implemented on all the servers in DHSGSU infrastructure:

- ☑ DHSGSU approved antivirus software for servers should be installed on all the servers.
- ☑ Update the virus signature regularly.
- ☑ Use centralized virus management for all the servers.

Email Antivirus Policy

Email is the common application used by the DHSGSU Faculty, Staff & Students and it is the most common means of virus outbreak, the email policy describes the procedures to limit the virus outbreak through email.

Configuration of Mail Server

Following policies are applicable to the exchange server installed in DHSGSU -

- ➢ DHSGSU approved antivirus software for exchange server should be installed on all the exchange servers.
- ➢ Antivirus software should be configured to scan all the incoming and outgoing mails.
- ➢ The sender and recipient should be notified about the virus if found in the mail.

- Antivirus software should be configured to update the virus signature daily.
- In case of a virus outbreak from a particular user, the user should be disabled till the virus is cured.
- IT team should be able to rapidly adjust the filtering rule in case of a virus outbreak.

Configuration of Mail Client

The mail client should be configured properly to prevent the virus outbreak in the network. User uses different mail client for accessing mail. DHSGSU supports three mail clients Outlook, Outlook Express, Netscape, Webmail (OWA), and Thunderbird

The following procedures are applicable to these clients only –

Outlook

- Set Internet Explorer security setting in the Internet Zone to high.
- Disable activex and active scripting.

Outlook Express

- Disable open and /or preview panes
- Set Internet Explorer security setting in the Internet Zone to high.

Netscape

- Disable java script.

Policies for all mail clients

All the mail clients should be configured to implement the following policies -

- Mail client should be configured for plain text only.
- Configure to challenge execution of all *.exe, *.hta, *.vbs and other executables.
- Configure to challenge opening of all *.doc and *.xls files.
- Turn off auto-open attachment.

Firewall Security Policy

A Firewall is a system (or network of systems) specially configured to control traffic between two networks. A Firewall can range from a simple packet filter, to multiple filters, dedicated proxy servers, logging computers, switches, hubs, routers and dedicated servers. A gateway or host is a secured computer system that provides access to certain applications. It cleans

outgoing traffic, restricts incoming traffic and may also hide the internal configuration from the outside.

Why Use a Firewall?

- Each external connection to the internal network should be secured so that it does not reduce the security of the internal network. The security of the network is only as secure as its weakest link.
- Every enterprise should have a firewall and/or security policy, and connections to external networks should conform to that policy. Normally, this is only possible through some kind of firewall.

- A firewall can stop confidential information from leaving a network and attackers from entering it.
- It can provide detailed statistics on communication between the networks (for example, who used what service and how often, as well as showing details of performance and bottlenecks).
- It can provide logging and audit trails of communications; the analysis of logs can be used to detect attacks and generate alarms.
- However, a strong firewall doesn't mean that the internal host security is no longer needed - on the contrary, most successful attacks come from insiders!
- Our policy is to take a widely used firewall solution and use it for all external connections.
- Examples of technical threats addressed by firewalls include IP spoofing, ICMP bombing, masquerading and attempts to gain access to weakly configured internal machines.
- Examples of risks reduced by firewalls are attacks from curious and malicious hackers, commercial espionage, accidental disclosure of company data (i.e. customer, employee and corporate data) and denial-of-service attacks.

Internet Firewall Policy

- **Access Control** - All internet access from the Institute network must pass over the situated firewall. The default configuration, unless otherwise specified, is that services are forbidden. All users are allowed to exchange emails in and out through the firewall. IT-Cell users are allowed to use www, ftp, https; others require authorisation.
- **Assurance** - Firewall machines are to be installed as sensitive hosts. All unnecessary services are to be stopped. Users should not be able directly to logon to these machines, but only through the IT-Cell's machines. The firewall policy and configuration must be accurately documented. The firewall machines must be subject to regular monitoring

and yearly audits. Users and Firewall administrators should be aware of their responsibilities and be educated so that they can assume these responsibilities.

- **Logging** - Detailed logs must be kept (where possible on a separate server). They should be automatically analysed, with critical errors generating alarms. Logs should be archived for at least six months and up to one year. The non-trivial log entries should be examined daily.
- **Availability** - The firewall must offer high availability and fulfil the resilience requirements (including backup/restores functions etc.) Processes exist for the change of management and incident response.

X. Network Security

DHSGSU computing and communication networks (wired and wireless) are part of DHSGSU's overall computing and communication infrastructure. Infrastructure is the underlying electronic information system hardware, software, and services that provide computing, information management, and communication capabilities to DHSGSU's departments, staffs, Students, and industry partners. DHSGSU computing and communication network is defined as the hardware and software components that support the movement of the institutes Information from one device to another. Examples of DHSGSU computing and communication networks include local area computing networks, wireless networks, telephone networks, and videoconference networks and CCTV surveillance network .The policy aims to enforce certain network controls so as to enhance the overall network security posture of DHSGSU.

The following are the controls for the DHSGSU computing and communication network configuration:

Wired Network

- Remote execution of DHSGSU computing and communication network security operations only within procedurally specified parameters and practices;
- Audit trails available and reviewed for all access attempts and configuration changes;
- A level of back-up in place for DHSGSU computing and communication network devices consistent with the level of risk and the impact on the DHSGSU's smooth functioning;
- Standardized protocols in place across the facility, with encryption capabilities and standards supported by the DHSGSU computing and communication network where appropriate;
- DHSGSU Information transmitted from any point within the DHSGSU computing and communication network and received only at the destination(s) it was intended to reach;

- DHSGSU Information received at any point within the DHSGSU computing and communication network exactly the same in content as the DHSGSU Information transmitted;
- Reasonable precautions implemented so that DHSGSU Information, while in transit, cannot be observed, tampered with, or extracted from the DHSGSU computing and communication network by some unauthorized person or device;
- Practices in place to identify any attempt to gain unauthorized access to the DHSGSU computing and communication network, so that appropriate corrective action can be taken (e.g. intrusion detection systems or system audit logs of unauthorized attempts);
- Alternate routes made available within the DHSGSU computing and communication network to provide for failure or deliberate destruction of any DHSGSU computing and communication network component (e.g. redundant links, device redundancy etc.)
- Other means of communication assured if both primary and back-up communication links are simultaneously unavailable, and this alternate tested;
- Technological diagnostic equipment (e.g., data scopes, line monitors) controlled to prevent unauthorized access to DHSGSU Information transmissions;
- Accurate, detailed, and current DHSGSU computing and communication network topology including the installed and applicable security measures maintained for all DHSGSU computing and communication network configurations. (Topology is the description of the locations of all DHSGSU computing and communication network components e.g., printers, personal computers, voice encryption devices). This documentation provides complete descriptions including:
    - Points of access,
    - DHSGSU computing and communication network devices, Communication protocols,
    - Physical location(s),
    - DHSGSU computing and communication network usage.
- All DHSGSU computing and communication networks must manage access when connecting to other internal and external computing and communication networks (e.g., firewalls) as specified by DHSGSU IT-Cell;
- Segregation of duties maintained for the performance of DHSGSU computing and communication network administration and security activities in both test and production environments.

Wireless Network (Wi-Fi) (802.11ac and 802.11ax WiFi)

Wireless local area network (WLAN) both 802.11ac vs 802.11ax Wi-Fi is deployed in entire campus of DHSGSU with controller for management and Aruba Clear Pass for MAC

authentication for each device on the network. Since it is Wi-Fi, we must understand and accept all risks associated with deploying a wireless system to the DHSGSU Network.

- WLANs must be tightly controlled and monitored to ensure that they are properly configured to meet minimum security standards.
- "Rogue" wireless access points must be immediately disconnected until they receive formal approval.

Requirements

- All wireless local area networks (WLANs) that transmit DHSGSU Information must meet the following minimum security requirements:
- DHSGSU wireless networks:
    - Be Wireless Protected Access (WPA) compliant
    - Be enabled with 802.1X/EAP-MS-PEAP for authentication and authorization
- All AP's(Access points) Manage with Wi-Fi Controller
  All the users are authenticated by Aruba ClearPass Tool
- Implement a separate VLAN for the WLAN compliant with DHSGSU network zoning requirements.
- Perform site surveys to ensure minimum RF leakage outside the intended environment.

Improperly configured WLANs pose many threats to the security of DHSGSU, including loss of confidential data, compromising of end systems, spreading of worms and viruses, etc.

XI. Cyber Crisis Management Plan

A) Purpose: The purpose of this plan is to establish the strategic framework and guide actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident.

B) Mandate: Ministries/Departments of Central Govt., State Govts. and Union Territories to draw-up their own sectoral Cyber Crisis Management Plans in line with the Cyber Crisis Management Plan for Countering Cyber-attacks and Cyber Terrorism.

C) Nature of Cyber Crisis and Contingencies:

- Cyber-attacks may be triggered on
    - Individual systems
    - Multiple systems and networks in a single or multiple organizations
    - States and entire Nation

- Targeted Scanning, Probing and Reconnaissance of Networks and IT Infrastructure
- Large scale defacement of websites
- Malicious Code attacks (virus/worm/ /Trojans/Botnets)
- Malware affecting Mobile devices
- Large scale SPAM attacks
- Identity Theft Attacks
- Denial of Service(DoS) attacks and Distributed Denial of Service(DDoS) attacks
- Domain Name Server (DNS) attacks
- Application Level Attacks
- Cyber Espionage and Advanced Persistent Threats

D) Prevention and Precautionary Measures

- Nomination of Chief Information Security Officer
- Information Security Policy & implementation of best practices
- Business Continuity Plan(BCP)
- Disaster Recovery Plan (DRP)
- Security of Information infrastructure and network
- Network traffic scanning
- Isolation of critical networks
- Implementation of Security guidelines issued by concerned authorities
- Background checks
- Audit & Assurance
- Security training & awareness
- Sharing of information pertaining to incidents

E) Incident Response and Mitigation

- Notify incidents to respective administrative
- Monitor and detect anomalous behavior and degradation of services
- Take all logs of affected systems for forensics analysis
- Notify and send relevant information to CERT-In/ NTRO/MoD, IDS (DIARA)
- Implement appropriate eradication process and recovery of systems as prescribed against each type of attack

THANKS

IT-Cell
Rupendra J. Chourasiya
Sr. System Analyst
(IT-Cell, Incharge)

Reference:

1. IT- IS Security Policies & Procedures For International Institute of Information Technology, Bangalore, Jan 2019

2. Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism. Indian Computer Emergency Response Team(CERT-In), Ministry of Electronics & Information Technology (MeitY)