

SOP for Maintenance



SGT UNIVERSITY

SHREE GURU GOBIND SINGH TRICENTENARY UNIVERSITY
GURGAON, DELHI-NCR

(Established by the Haryana Act No. 8 of 2013)

Office of GM (Administration)

Standard Operating Procedures for the Maintenance of Classrooms/Hostels/Buildings/Labs

Scope:-

This document describes the SOP for maintenance of all facilities located in the campus of SGT University.

Maintenance of Classrooms

1. The classrooms are cleaned daily by the Housekeeping Staff and the cleanliness is supervised by concerned supervisor/admin In-charge of the building.
2. The scavenging of the benches in the classrooms is also done by the Housekeeping Staff
3. The maintenance of the classrooms is done on regular basis
4. Building In-charges are responsible for the overall cleaning /scavenging and if there is any problem, the same is brought forward to the knowledge of GM (Admin) and corrective measures are taken to correct/rectify the same.

Maintenance of Restrooms

1. The cleaning/scavenging of the restrooms is done by the staff appointed by the SGT University.
2. The Admin In-charge of the building is responsible for supervising to ensure the regular cleaning/scavenging of the restrooms.
3. If there is any breakage of furniture/ fixture, the same is reported by the Admin In -charge to the concerned department for repair/replacement as the case may be.
4. The appropriate boards with proper instructions for usages and maintenance of the restrooms are displayed.

Maintenance of Fire Extinguishing Equipments

1. The staff to look after the day to day problems has been appointed by SGT University.
2. The services of the fire equipments is carried out by the External Service Provider(ESP).
3. The equipments are maintained by fire department of the University.
4. Major maintenance if any is also done by External Service Provider(ESP) under annual maintenance contract.

Maintenance of Labs

1. Maintenance of all labs and equipments is done under the supervision of lab technician and admin In-charge of that particular block/faculty of the University.
2. Annual maintenance of all equipments is done by ESP and obsolete equipment /parts are replaced with latest equipments.

Registrar
SGT University
Budhera, Gurugram

Pest Control

1. Pest Control is carried out on a regular basis by in-house team under Maintenance department of the University.
2. Any reported incidence of pests is treated on priority.

Laundry Services

1. University provides laundry services to all the stake holders within the campus.
2. There is complete in-house laundry unit for washing and ironing purpose which is maintained by the university itself.

Maintenance of Hostels

1. The residents of the hostel (students) identify the problem and record their complaint in the complaint register maintained in the office of the warden.
2. The complaints given by the students are reported to maintenance department who in turn depute the concerned staff for execution the repair work.
3. Major repair if any is executed by the project department of the University. The project department is equipped with trained and qualified staff and essential equipments.
4. Follow up action is always done to ensure the promptness in carrying out the repair work.
5. Record of all the complaints and execution of the repair work is maintained.

Cleanliness of the Hostel

1. Each room of the students is cleaned by the Housekeeping Staff. The area surrounding the hostel is also cleaned by the Housekeeping Staff.
2. The proper record of cleaning the toilets in the hostel is kept by the Housekeeping Supervisor and the same is maintained regularly.
3. The other facilities like gym and sports facility are maintained by University under the supervision of the Hostel Warden.

Warden (Administration)

He/ She will allot hostel rooms only after ensuring the payment of hostel fee copy of the receipt must be prepared in the record.

1. He/ She will check the resident students register and the guest room register.
2. He/ She will take disciplinary action for keeping any unauthorized guest.
3. He/ She will order double-locking of rooms of resident students and their re-opening, when required.
4. He/ She will be responsible for the overall security of the hostel and will coordinate his/her responsibility with the Security Officer of the University.
5. He/ She will periodically verify the furniture and fittings of the hostel with the assistance of the Caretaker, and take action for their repairs/replacement or for obtaining additional furniture.


Registrar
SGT University
Budhera, Gurugram

Warden (Health & Recreation):

He/ She will be responsible for general matters relating to health with the advice of the Chief Medical Officer (CMO).

1. He/ She will look after the common room and the sports and cultural programmes of the hostel and will regulate disbursements out of the hostel's recreation grant.
2. He/ She will check the bills prepared by the Caretaker for purchase of Newspapers and Magazines.
3. He/ She will arrange disposal of old Newspapers and Magazines and ensure that the sale proceeds are deposited in the appropriate head of account.
4. He/ She will ensure maintenance of discipline and decorum in the common room.
5. He/ She can permit the common room to stay open beyond the prescribed hour on a special occasion.
6. He/ She will pursue, at appropriate level, all complaints relating to common room items like television.

Warden (Sanitation & Maintenance):

1. He/She will be responsible for all matters relating to hygiene, sanitation and cleanliness of the hostel in consultation with/ upon the advice of the CMO.
2. He/She will supervise the work of the sanitation staff, keep a control over their attendance and maintain the Attendance Register.
3. He/She can grant Casual Leave to the sanitation staff and recommend regular leave to the Chief warden/GM(Admin) as per delegation of authority given in the Manual.
4. He/She shall ensure implementation of the Minimum Wage Act and other contractual obligations by the private manpower service provider towards the sanitary staff under contract.

Warden (Mess):

1. With the assistance of the Mess Committee, he/she will supervise the functioning of the mess and the working of the Supervisors, Cooks and Helpers under his/her charge.
2. He/She will keep a watch over the cleanliness of the dining hall and the kitchen and of the food prepared.
3. He/She will conduct regular inspection of the kitchen room and the dining hall, especially when the residents take their meals.
4. He/She will enforce discipline and decorum in the dining hall.
5. He/She will supervise the system of purchases of mess stores, provision etc.

6. He/She will ensure the correctness of receipts and issues of mess stores, crockery etc. and of the stock balance and will attest all entries in the relevant stock register. Will check the valuation of the closing stock.

7. He/She will ensure that stores are kept in good and efficient condition.

He/She will stop mess facilities in respect of residents defaulting payment of mess bills and recommend action to the Chief Warden for eviction.

8. He/She will stop mess facilities in respect of those who have vacated the hostel or have been evicted.


9. He/She will supervise the deployment of Cooks and Helpers on daily wage and overtime when necessary as per rules.

Wet Waste Management

1. The Institution has placed separate bins to collect dry and wet waste in different parts of the campus.
2. The institution has appointed ESP to collect the dry and wet waste from the bins located in the campus and dump the waste on a daily basis.
3. The waste management is done in accordance with local policy & regulations of Govt. agencies

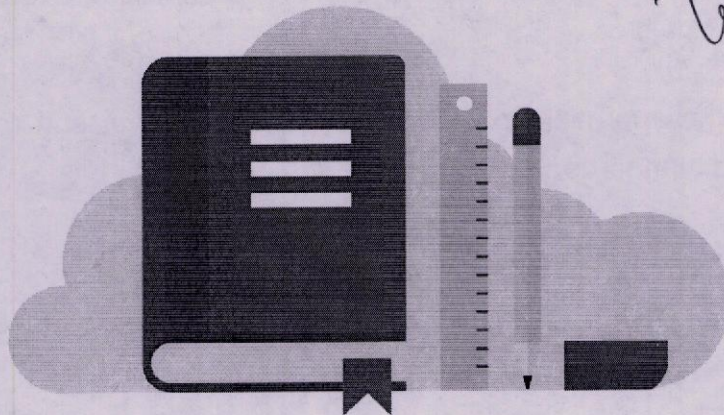
E- Waste Management

1. The Institution has a designated storage space for temporarily storing all electronic waste.
2. The institution has appointed an ESP to collect the e-waste


General Manager (Admin)
SGT University, Gurugram


Registrar
SGT University
Budhera, Gurugram

Teller him



SGT University

IT Policy and SOPs

Contents :

IT POLICY AND STANDARD LIFE
CYCLE

POLICY AND STANDARD
LIFECYCLE

ACCEPTABLE USE

EMAIL

INFORMATION SECURITY

IDENTITY AND PASSWORDS

INTELLECTUAL PROPERTY



A handwritten signature in blue ink, appearing to be a stylized 'V' or similar character.

Registrar
SGT University
Budhera, Gurugram

Purpose

To define the approach to the development, approval and maintenance of IT policies and standards.

Scope

This applies to all policies and standards recommended by governance for SGTU and issued by IT Department.

Standard

Policy and standard development and approval

1. Any faculty, staff member or student may propose a topic or content for a policy or standard. Such proposals should be directed to the relevant topical committee or to the Office of the Information Technology.
2. The chair of each topical committee decides which proposals are appropriate for consideration
3. Drafts of proposals to be considered are typically prepared by staff and submitted to the topical committee. The topical committee reviews and modifies the draft as needed, and makes a recommendation to the IT Department. The topical committee may seek input from constituent groups
4. IT Department will review the draft. The draft can be returned to the originating committee with comments for modification or forwarded to other committees or constituents for comment
5. Comments are returned to the originating committee, which addresses the comments and makes a recommendation to the IT Department.
6. IT Department seeks input from University administration and others as appropriate
7. IT Department seeks input from the Office of General Counsel
8. The Vice Chancellor approves the policy or standard

Policy and standard implementation

Registrar
SGT University
Budhewa
Program

1. The Registrar Office notifies the University by issuing a DDD about the new policy or standard and its effective date
2. Policies and standards are posted on the SGTU website
3. Information about policies and standards may also be communicated via announcements, memoranda and training

Policy and standard maintenance

1. Revisions to policies and standards follow the same process for approval as new policies or standards
2. Policies and standards should be reviewed as appropriate or as required by law

ACCEPTABLE USE POLICY

PROCEDURE FOR MONITORING OF IT RESOURCES

This represents a summary of the University's Acceptable Use Policy. Users are required to comply with the full policy, which details the approval requirements.

Introduction

University Information Technology (IT) resources are to be used for university-related purposes. Some examples of IT resources are computers, software, networks, and electronic devices. This policy applies to all users of university IT resources, whether affiliated with the university or not, and to all users of those resources, whether on campus or from remote locations. Users are responsible for following the University's Acceptable Use Policy.

General Rules


Registrar
SGT University
Budhera, Gurugram

-
1. Users of university IT resources must comply with all applicable legal requirements.
 2. Users are responsible for any activity originating from their accounts. Users shall not share their accounts and passwords.
 3. Users shall not use IT resources to gain unauthorized access to anything.
 4. Disruptive use of university IT resources is not permitted.
 5. University IT resources shall not to be used for commercial purposes without prior approval.
 6. Occasional personal use of university IT resources by employees is permitted when it does not consume a significant amount of those resources, is otherwise in compliance with this policy, and meets with the approval of the supervisor.
 7. The university may monitor the activity and accounts of any users of university IT resources.
 8. Communications made concerning university business are generally subject to the Indian Constitutional Law and retention requirements.
 9. Users must not augment the university network infrastructure without prior approval.

Additional requirements apply to the collection, use, storage, and maintenance of Restricted Data.

Consequences of Violations

Users who violate this policy may be subject to penalties and disciplinary action, including expulsion, dismissal, or revocation of user acc

ACCEPTABLE USE POLICY



Registrar
SGT University
Buddha, Gurugram

Introduction


As part of its educational mission, the SGTU acquires, develops, and maintains computers, computer systems and networks. These Information Technology (IT) resources are intended for university-related purposes, including direct and indirect support of the university's instruction, research and service missions; university administrative functions; student and campus life activities; and the free exchange of ideas within the university community and among the university community and the wider local, national, and world communities.

This policy applies to all users of university IT resources, whether affiliated with the university or not, and to all uses of those resources, whether on campus or from remote locations. This policy may be modified as deemed appropriate by the University. Users are encouraged to periodically review the policy as posted on the university's home page.

General Rules

Users of university IT resources must comply with Indian Constitutional Law, university rules, regulations and policies, and the terms of applicable contracts including software licenses while using university IT resources. Examples of applicable laws, rules and policies include but are not limited to the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the Computer Crimes Act, the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking" and similar activities; the university's Student Code of Conduct; the university's Sexual Harassment Policy; the University's Policy on the Use of the University Name and Logos, the University's Web Page policy, and the University's E-mail Policy. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks. Users with questions as to how the various laws, rules and regulations may apply to a particular use of university computing resources should contact the Office of the General Counsel for more information.

Users are responsible for ascertaining what authorizations are necessary and for obtaining them before using university IT resources. Users are responsible for any


Registrar
SGT University
Budhera, Gurugram

activity originating from their accounts which they can reasonably be expected to control. Accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned by the account administrator. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident to the appropriate account administrator, Unit Information Security Manager, and/or Dean, Director, or Department Chair.

Disruptive use of university IT resources is not permitted. Units administering the resources involved will determine whether specific usage is considered normal, excessive or disruptive. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of university IT resources, the university may require users of those resources to limit or refrain from specific uses if such use interferes with the efficient operations of the system.

Users may not use IT resources to gain unauthorized access to remote computers or to impair or damage the operations of SGTU computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or sniffing communications, and running, installing or sharing virus programs. Deliberate attempts to circumvent data protection or other security measures are prohibited.

Users who violate this policy may be denied access to university IT resources. The university may suspend, block or restrict access to an account when it appears necessary to do so: a) to protect the integrity, security, or functionality of university or other IT resources; b) to comply with legal or contractual requirements; c) to investigate alleged or potential violations of law or policy including, without limitation, state, federal, or local law, or university or Board of Governors rules, regulations, policies, or collective bargaining agreements; d) to investigate any asserted, threatened or potential complaint or grievance filed or credibly alleged pursuant to law or university or Board of Governors rules, regulations, policies, or collective bargaining agreements, or subject of law enforcement review or investigation; e) or to protect the university from liability or disruption. The university may also refer suspected violations of law to appropriate law enforcement agencies for further investigation or action.



Registrar
SGT University
Budhera, Gurugram

Users who violate the Policy may be subject to other penalties and disciplinary action, including expulsion or dismissal, under applicable university or Board of Governors rules, regulations, policies, or collective bargaining agreements.

Security, Privacy, and Public Records

The university employs various measures to protect the security of its IT resources and user accounts. However the university cannot guarantee complete security and confidentiality. It is the responsibility of users to practice "safe computing" by establishing appropriate access restrictions for their accounts, by guarding their passwords, and by changing them regularly.

Users should also be aware that their use of university IT resources is not private. While the university does not routinely monitor individual usage of its IT resources, the normal operation and maintenance of the university's IT resources require the backup and caching of data and communications, the logging of activity, monitoring of general usage patterns and other activities necessary or convenient for the provision of service.

The university may monitor SGTU resources and retrieve communications and other records of specific users of SGTU resources, including individual login sessions and the content of individual communications, without notice. The criteria and steps required for approval of such monitoring or retrieval without notice are set forth in the policy on the Monitoring of University Information Technology Resources and Retrieval of Communications.

Communications made by means of university IT resources are also generally subject to the same extent as they would be if made on paper. In this regard, university personnel and agents should be aware that most written communications concerning university matters, regardless of whether university computing resources are used, are public records, many of which are disclosable to the public upon request. Public records requests must be referred to the Registrar Office for coordinating the response and review of requirements and exemptions.

Retention periods must be followed for all university records and communications as required by Law and any other applicable law or contractual requirements.


Registrar
SGT University
Budhera, Gurugram

Commercial Use

IT resources are not to be used for personal commercial purposes or for personal financial or other gain. Occasional personal use of university IT resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other university responsibilities, and is otherwise in compliance with this and other university policies, including without limitation the university's policies on outside activities and use of University trademarks and names. Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of University equipment.

Network Infrastructure/Routing and Wireless Media

Users must not implement their own network infrastructure. This includes, but is not limited to basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. Users must not offer alternate methods of access to SGTU resources such as modems and virtual private networks (VPNs). Users must not offer network infrastructure services such as DHCP and DNS.

Wireless is shared media and easily intercepted by a third party. Wireless users are encouraged to use some type of encryption.

PROCEDURE FOR MONITORING OF IT RESOURCES

The University may monitor SGTU resources and retrieve communications and other records of specific users of SGTU resources, including individual login session and the content of individual communications, without notice. The criteria and steps required for approval of such monitoring or retrieval without notice are set forth in this policy.

A request for such monitoring or retrieval of records and documents must be provided to IT Department with the necessary approvals. Approvals must be obtained from the General Counsel (or designee) and the IT Head who supervises the unit requesting such access. If the records are being monitored or retrieved for the purposes of reviewing or investigating employee conduct, the approval of the General Manager for Human Resource Services is also required.


Registrar
SGT University
Budhera, Gurugram

Prior approval is not required to monitor SGTU resources or retrieve communications and other records in the following situations:

The communications and/or records have been made accessible to the public, as by posting to a webpage.

A person's authorization to access or use any SGTU resources ends, for example upon termination of SGTU employment or appointment.

The monitoring or retrieval is in response to an emergency. An emergency occurs when there is an imminent threat to life or property and there is not sufficient time available to obtain approval. In such a situation, monitoring or retrieval may be conducted without prior approval, with notification to the appropriate University Official as soon as possible. The scope of access should be reasonable in relation to the emergency situation involved.

Approval may be granted to monitor communications or retrieve records when any one or more of the following situations apply:

It reasonably appears necessary or appropriate to do so to protect the integrity, security or functionality of university or other computing resources.

It reasonably appears necessary or appropriate to do so to comply with legal or contractual requirements or to protect the university from liability or disruption. Examples of situations in which access and retrieval are authorized under this paragraph include but are not limited to responses to public records requests, subpoenas, court orders, and discovery requests,

There is reasonable cause to believe that the user has violated or is violating the Acceptable Use Policy or that the user has violated, or is violating, any other university or Board of Governors rule, regulation, policy, or collective bargaining agreement, or any other law or regulation and the access is reasonable in relation to the believed violation.

It is part of any investigation or review of an already asserted, threatened or potential complaint or grievance or of a credible allegation of a violation of the law, including without limitation local, state or federal law, or foreign law as applicable, or university or Board of Governors rule, regulation or policy, or the subject of a law


Registrar
SGT University
Budhera, Gurugram

enforcement review or investigation, and the scope of access to the account or activity is reasonable in relation to the complaint, grievance or allegation.

An account appears to be engaged in unusual or unusually excessive activity.

The University has a legitimate need to access an account or activity and the access is reasonable in relation to the need.

The results of any such general or individual monitoring, including but not limited to the contents and records of individual communications, may be released pursuant to a public records request. In addition, the university, in its discretion, may disclose the results of any such general or individual monitoring for any legitimate purpose to appropriate university personnel or law enforcement agencies and may use those results in appropriate external and internal disciplinary and other proceedings.

EIT POLICY

PURPOSE:


This policy establishes standards for Electronic Information Technology (EIT) accessibility in compliance with applicable local, state and federal regulations and laws. The SGT University is committed to providing equal access to its services, programs, and activities for all users. An accessible EIT environment enhances usability for everyone.

SCOPE:

This policy applies to all EIT acquired, developed, distributed, used, purchased or implemented by or for the University and used to provide University programs, services, or activities. This includes, but is not limited to, all EIT related to University business, academic and outreach, including web pages that represent the University, electronic documents and any multimedia created or obtained.

POLICY:

The University adopts the World Wide Web Consortium's standard: Web Content Accessibility Guidelines (WCAG) Version 2.0, AA conformance level as the minimum accessibility standard for all EIT, and Guidance on Applying WCAG 2.0


Registrar
SGT University
Budhera, Gurugram

to Non-Web Information and Communications Technologies (WCAG2ICT). In addition, all EIT shall comply with federal and state laws.

SGTU Policy on E-Mail as Public Records

It is the policy of SGTU that all employees will comply with SGT's public records law and state retention schedules for public records, including electronic mail (e-mail).

SGTU's Public Records Law:

"All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software or other material, regardless of physical form, or characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency."

How the Law Affects You as a SGTU Employee:

E-mail created or received by SGT University employees in connection with official business, which perpetuates, communicates or formalizes knowledge, is subject to the public records law and open for inspection.

If your e-mail falls within the definition of a public record, you may not delete it except as provided in the university's record retention schedule . Unless it falls within one of the specific exemptions described in the public records statute, you must produce that e-mail message to any person upon request. A person need not have a "legitimate" need for public records to be entitled to inspect them.

Exemptions to the Public Records Law:

Country law exempts certain categories of documents from disclosure under the public records law. The exemptions which apply most often to SGT University records include:


Registrar
SGT University
Budhera, Gurugram

Certain documents involving personnel matters, which are confidential under law;

Student records which, except for "directory information," must be kept confidential pursuant to the Buckley Amendment; and

Certain kinds of research records that are confidential under law.

Before any e-mail is released pursuant to a public records request, any exempt information must be deleted from the e-mail.

Responding to a Public Records Request:

Public records requests may be made in writing or orally. All public records requests should be referred to the appropriate department chair or administrative supervisor. The department chair or administrative supervisor is responsible for appointing one or more persons to gather the requested documents and then either arranging a time for inspection of the documents or making copies available to the requestor. E-mail that does not fall within the definition of a public record should not be produced. E-mail which is a public record but contains exempt information should be produced but the exempt information must first be deleted or redacted. If in doubt as to whether an e-mail message is a public record or contains exempt information, the department chair or administrative supervisor should contact the Office of Registrar, which will consult with the Management as necessary.

If the person making the records request wishes to obtain copies of the documents, the public records law allows the university to charge 15 cents per one-sided copy. In addition, if copying the public records requires extensive use of information technology resources or clerical and/or supervisory assistance, the university may assess a reasonable service charge based on the university's actual incurred costs. An estimate of the charges should be given to the requestor and approval obtained prior to responding to the request. All charges should be collected before producing the documents.

Transitory Messages



Registrar
SGT University
Budhera, Gurugram

The record series entitled "Transitory Messages," found in the university's general records schedule, is designed to cover certain E-mail communications, as well as other information with short-term administrative value. The transitory message series is defined as follows:

Transitory messages consist of those records that are created primarily for the informal communication of information, as opposed to communications designed for the perpetuation or formalization of knowledge. Transitory messages do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt. The informal nature of transitory messages might be compared to the communication that might take place during a telephone conversation or verbal communications in an office hallway. Transitory messages would include, but would not be limited to: E-mail messages with short-lived or no administrative value, voice mail, self-sticking notes, and telephone messages.

Retention is defined as retaining until obsolete, superseded, or administrative value is lost.

Retention Periods for Public Records:

Retention periods for public records, including e-mail, can be found in the university's general records schedule. This schedule incorporates items found in the state General Records Schedule for State and Local Government Records (GS1), University/Community College Records (GS5) and other SGT University retention schedules. The university's general records schedule is available in the Records Management Office.

Retention schedules are based on a record's informational content, not its format. Retention of most e-mail records falls within the following two categories:

1. Retain Until Obsolete, Superseded, or Administrative Value is Lost: This means that the records only have to be retained until they have served their administrative purpose. Examples of such records would be as follows:

Transitory Messages as defined above.



Registrar
SGT University
Budhera, Gurugram

Routine announcements and information, including notices of seminars or workshops, queries regarding processes or ideas, and general information regarding programs.

Reference files that are general information files used in daily functions of the administrative area.

Meeting notices, statistical records, reading files, and recipients' inter-departmental memoranda.

2. Retain for Three Fiscal Years: General correspondence, sender's inter-departmental memoranda, and most fiscal and budget records.

Each year, administrative offices are required to file records disposition requests with the Records Management Office for any obsolete public records that they wish to destroy. E-mail files should be a part of these destruction requests.

However, University allows state agencies to dispose of all records with a retention value of, "retain until obsolete, superceded, or administrative value lost"(OSA) without having to fill out a records disposition request. In other words, both duplicates and master copies of records with this retention period may be disposed of by each department when, in the judgement of the department, they are obsolete, superceded, or have lost their administrative value. In applying this rule, any E-mail messages created or received that fall under this retention period may be deleted at the user's discretion, under the above standards.

E-mail messages that have a longer retention period -- such as correspondence or sender's memoranda -- must be kept through the three-year retention period and may not be disposed of until records disposition requests have been submitted and approved.

Maintaining E-Mail Documents:

Florida's public records law offers challenges to maintaining e-mail, mainly because e-mail documents are both informal and efficient. Most e-mail users prefer to reduce or eliminate the handling, filing and archiving tasks often associated with hard copy. Because of the differences in which e-mail and hard

copy are used, many e-mail users do not have systems in place for periodically reviewing, storing or deleting e-mail.

Public record e-mail can be deleted after it has been retained for the correct time period as determined by the retention schedules. A public record that is stored and accessible after this time is still a public record and must be produced upon request. A systematic deletion program not only eliminates obsolete documents from the file, but also saves resources by not indefinitely and unnecessarily storing information beyond appropriate time lines.

While methods for reviewing, storing or deleting e-mail vary, you can comply with the retention requirements of the public records law by doing one of the following:

Print the e-mail and store the hard copy in the relevant subject matter file as you would any other hard-copy communication. Printing the e-mail permits you to keep all information on a particular subject matter in one central location, enhancing its historical and archival value. If you choose this method, you may wish to set up your e-mail account so that it does not log outgoing e-mail by default. This will require you to not only print each public record message you send but also determine when you send the e-mail whether it must be saved under the public records law. You must also determine if incoming e-mail must also be printed before being deleted from your system.

Electronically store your public record e-mail according to the conventions of your e-mail system and retain it electronically pursuant to the university's retention schedules.

The technical details and methods of storing, retrieving and printing your e-mail depend on the e-mail system you use. Consult with your IT Manager, or departmental computer support personnel, for details.

Some automatic periodic backup of e-mail by university and department system administrators is done under the university's disaster recovery plan. It is not designed to comply with the public records law. Thus, you need to set up your own retention procedures as outlined above to be sure you are in compliance with the law.


Registrar
SGT University
Budhera, Gurugram

The previously listed methods for retaining e-mail are in compliance with the public records law. Regardless of the method used, remember: the ultimate responsibility for complying with the public records law is on you, the e-mail user.

SPAM POLICY

Introduction

This policy is targeted at sources of unwanted, unsolicited email (spam) external to the SGTU Network.

Spam sent to University accounts is unacceptable and violates the terms of acceptable use of the University IT resources. It disrupts the public workplace, is detrimental to our resources, and it is not welcome by our users.

Enforcement

After the first occurrence, an attempt will be made to notify the sender that unsolicited email should not be sent to university accounts and that any further receipt of such messages will initiate our procedures to block email from the sender.

After the second occurrence, the system will be configured to block email coming from the offending account. Any reinstatement of privileges must be requested in writing from the SGTU.

ELECTRONIC MAIL

Purpose

To provide for compliance, security, and efficient support services when conducting SGTU business via electronic mail.

Scope

This policy applies to all electronic mail sent or received in the scope of employment at the university, or with the intention to conduct university business.

Policy



Registrar
SGT University
Budhera, Gurugram

All employees of the University must use a university provided or approved electronic mail service (Email ID) when conducting University business via electronic mail.

SGT University electronic mail may not be automatically forwarded to a non-university provided or approved service.

SGT University business must be conducted using an assigned sgtuniversity.org email address.

Responsibilities

1. All SGT University faculty and staff are responsible for compliance with this policy

MOBILE COMPUTING AND STORAGE DEVICES POLICY

Purpose

To ensure secure, reliable, and accountable use of mobile computing and storage devices with University Restricted Data. This policy establishes unified management, and formally assigns roles and responsibilities for these devices.

Scope

This policy applies to all mobile computing and storage devices used by the University constituency in the performance of their duties, and to all University Restricted Data when accessed through, or stored on, mobile computing and storage devices, regardless of the device's ownership. University Restricted Data may not be released for storage on or access through, devices that do not meet these requirements.


Registrar
SGT University
Budhera, Gurugram

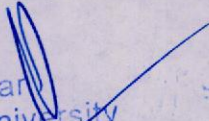
Policy

All mobile computing and storage devices that access the University Intranet and/or store University Restricted data must be compliant with University Information Security Policies and Standards.

1. Restricted Data stored on mobile computing and storage devices must be encrypted.
2. Any and all mobile computing devices used within the University information and computing environments must meet all applicable SGTU encryption standards. mobile computing devices purchased with University funds, including, but not limited to contracts, grants, and gifts, must also be recorded in the unit's information assets inventory.
3. University information security policies applicable to desktop or workstation computers apply to mobile computing devices.

Responsibilities

1. The University Information Security and Compliance Office will establish standards to govern the secure use of all mobile computing and storage devices at the University.
2. The SGTU Office of the Registrar will provide guidance to assist units in complying with these requirements.
3. All University deans, directors and department chairs, in conjunction with their IT support teams, are responsible for migrating all existing uses of mobile computing and storage devices within their areas of responsibility to devices and services that are compliant with university policies and standards.
4. All members of the University constituency who are currently using personally owned mobile computing and storage devices that access the University Intranet and/or store SGTU Restricted Data are required to bring their personal device into compliance with the SGTU Information Security Standard for Mobile Computing and Storage Devices.
5. All members of the SGTU constituency will report the loss or theft of a mobile computing or storage device to their departmental Information Security Manager


Registrar
SGT University
Budhera, Gurugram

(ISM) immediately upon detection of the loss. The SGTU Privacy Office must be immediately notified of theft or loss of any portable computing device or media that contains Restricted Data.

DATA CLASSIFICATION POLICY

DATA CLASSIFICATION POLICY

AUTHENTICATION MANAGEMENT POLICY

RISK MANAGEMENT POLICY

ACCOUNT MANAGEMENT POLICY

BACKUP AND RECOVERY

RELATED STANDARDS AND DOCUMENTS

REMOTE ACCESS POLICY

REMOTE ACCESS STANDARD

MEDIA SANITIZATION STANDARD

AUDITABLE EVENTS AND RECORD CONTENT STANDARD

AUDIT AND LOGGING POLICY

CONTROL OF ELECTRONIC MEDIA

Purpose

To provide the basis for protecting the confidentiality of data at the SGTU by establishing a data classification system. Further policies and standards will specify handling requirements for data based on their classification.

Scope

This standard applies to all data or information that is created, collected, stored or processed by the University, in electronic or non-electronic formats.

Registrar
SGT University
Budhara, Gurugram

Policy

All data at the SGTU shall be assigned one of the following classifications. Collections of diverse information should be classified as to the most secure classification level of an individual information component with the aggregated information.

1. Restricted: Data in any format collected, developed, maintained or managed by or on behalf of the university, or within the scope of university activities that are subject to specific protections under law or regulations or under applicable contracts. Examples include, but are not limited to medical records, social security numbers, credit card numbers, driver licenses, non-directory student records and export controlled technical data.
2. Sensitive: Data whose loss or unauthorized disclosure would impair the functions of the university, cause significant financial or reputational loss or lead to likely legal liability. Examples include, but are not limited to, research work in progress, animal research protocols, financial information, strategy documents and information used to secure the university's physical or information environment.
3. Open: Data that does not fall into any of the other information classifications. This data may be made generally available without specific information owner's designee or delegate approval. Examples include, but are not limited to, advertisements, job opening announcements, university catalogs, regulations and policies, faculty publication titles and press releases.

Responsibilities

1. Data owners are responsible for appropriately classifying data.
2. Data custodians are responsible for labeling data with the appropriate classification and applying required and suggested safeguards.
3. Data users are responsible for complying with data use requirements.
4. Data users are responsible for immediately referring requests for public records to the University Relations Division – Office of Public Affairs or to the Office of the Vice President and General Counsel.

Registrar
SGT University
Budhera, Gurugram

AUTHENTICATION MANAGEMENT POLICY

PURPOSE

Authentication mechanisms such as passwords are the primary means of protecting access to computer systems and data. It is essential that these authenticators be strongly constructed and used in a manner that prevents their compromise.

SCOPE:

This policy applies to all passwords and other authentication methods used at the university.

POLICY:

1. Access to all university data and systems not intended for unrestricted public access requires authentication.
2. Passwords and other authenticators must be constructed to have a resistance to attack commensurate with the level of system or data access granted to the account.
3. Systems must be designed and configured to protect passwords during storage and transmission.
4. No one may require another to share the password to an individually assigned university account, for example as a condition of employment or in order to provide technical support.

RESPONSIBILITIES:

1. All members of the SGTU Constituency are responsible for any activity that occurs as a result of the use of authentication methods issued to them.
2. All members of the SGTU Constituency are responsible for protecting the password or authentication method associated with an individually assigned university account. Passwords may not be shared or disclosed to anyone else.

3. All members of the SGTU Constituency are responsible for reporting any suspicious use of assigned authentication mechanisms. Anyone that reasonably believes his or her password to be known by anyone else must change it immediately. Lost or stolen authentication devices are to be reported immediately.

4. Information Security Managers (ISM) are responsible for verifying that information systems under their control, and those intended for acquisition or development by their unit, comply with this policy.

5. IT Manager is responsible for implementing systems and specifications to facilitate unit compliance with this policy.

RISK MANAGEMENT POLICY

PURPOSE

To establish a process to manage risks to the SGTU that result from threats to the confidentiality, integrity and availability of University Data and Information Systems.

SCOPE:

This policy applies to all electronic data created, stored, processed or transmitted by the SGTU, and the Information Systems used with that data.

POLICY:

1. All Information Systems must be assessed for risk to the SGTU that results from threats to the integrity, availability and confidentiality of SGTU Data. Assessments must be completed prior to purchase of, or significant changes to, an Information System; and at least every 2 years for systems that store, process or transmit Restricted Data.
2. Risks identified by a risk assessment must be mitigated or accepted prior to the system being placed into operation.

Registrar
SGT University
Budhera, Gurugram

3. Residual risks may only be accepted on behalf of the university by a person with the appropriate level of authority as determined by University. Approval authority may be delegated if documented in writing, but ultimate responsibility for risk acceptance cannot be delegated.

4. Each Information System must have a system security plan, prepared using input from risk, security and vulnerability assessments.

RESPONSIBILITIES:

1. Information Security Administrators (ISAs) are responsible for ensuring that their unit conducts risk assessments on Information Systems, and uses the university approved process.

2. Information Security Managers (ISMs) are responsible for assessing and mitigating risks using the university approved process.

3. Information System Owners (ISOs) are responsible for ensuring that information systems under their control are assessed for risk and that identified risks are mitigated, transferred or accepted.

4. IT Department is responsible for implementing systems and specifications to facilitate unit compliance with this policy.

ACCOUNT MANAGEMENT POLICY

PURPOSE

To provide a comprehensive account management process that allows only authorized individuals access to University Data and Information Systems.

SCOPE:

This policy applies to all Information Systems, University Data, identities and accounts used to access them and University Data.


Registrar
SGT University
Budhera, Gurugram

POLICY:

1. All persons and processes granted access to an information system, beyond that explicitly intended for unauthenticated public access must be uniquely and individually identified and authenticated.
2. All persons and processes that have been granted access to an information system must have an approved and documented level and scope of access.
3. Access to University Data and Information Systems is to be promptly modified upon changes in university affiliation, position, or responsibilities.

RESPONSIBILITIES:

1. All members of the University Constituency are responsible for all actions initiated from accounts issued to them.
2. Managers of university employees are responsible for promptly coordinating suspension of accounts for terminated employees.
3. Information Security Administrators (ISAs) are responsible for developing and implementing procedures to properly authorize, modify or terminate accounts and permissions.
4. Information Security Managers (ISMs) are responsible for implementing Information Systems such that account authorizations are promptly enforced.

BACKUP AND RECOVERY**PURPOSE**

The purpose of this policy is to protect University Data from loss or destruction by specifying reliable backups that are based upon the availability needs of each unit and its data.

SCOPE

This policy applies to all SGTU Data and the Information Systems used with it.

POLICY

Registrar
SGT University
Budhera, Gurugram

University Data is backed up in a manner sufficient to restore any or all of an Information System in the event of a data loss, according to Recovery Time Objectives and Recovery Point Objectives.

Backups are periodically tested to ensure that backups are sufficient and reliable.

Backup systems and media protect the confidentiality, integrity and availability of stored data.

Written procedures are maintained to allow unit personnel to recover data in the event of an emergency.

RESPONSIBILITIES

1. Information Security Administrators (ISAs) are responsible for establishing Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), in conjunction with data users and owners, for all University Data collected, stored or maintained by the unit. ISAs should verify that Data used by the unit, but collected, stored or maintained by others, have appropriate backup plans.
2. Information Security Managers (ISMs) are responsible for implementing backup systems and processes to ensure that RTO and RPO can be met for all data collected, stored or maintained on unit Information Systems. ISMs document backup system operation and test recovery capability.
3. IT Department is responsible for implementing systems and specifications to facilitate unit compliance with this policy.

SGTU INFORMATION TECHNOLOGY SECURITY CHARTER

Introduction

This charter defines the mission and objectives of the SGTU Information Technology (IT) security program, outlines the scope of the organization's mandate, defines terms, and delineates roles and responsibilities for information security throughout the organization. Enforcement rules are also included in this charter.


Registrar
SGT University
Budhera, Gurugram

Unauthorized access, breach of confidentiality, loss of integrity, disruption of availability, and other risks threaten SGTU IT resources. SGTU IT security policies are aimed at reducing exposure to threats, thereby minimizing risk in order to protect SGTU IT resources. Policies are goals or mandates used to cultivate standards. SGTU IT security standards define metrics against which results can be measured to determine compliance with the policies and describe objectives for procedures. SGTU IT security procedures detail how to implement standards in order to comply with policies. Guidelines are suggested methods, best practices, or clarifications to assist with the implementation of standards.

Mission and Objectives

As part of its educational mission and strategic plan to provide state-of-the-art information technology to meet the needs of faculty and students in research and teaching, the SGTU acquires, develops, and maintains data and information, computers, computer systems and networks. These information technology (IT) resources are intended for university related purposes, including direct and indirect support of the university's instruction, research and service missions; university administrative functions; student and campus life activities; and the free exchange of ideas within the university community and among the university community and the wider local, national, and world communities.

The mission of the SGTU information security program is to support the goals of SGTU by assuring the availability, integrity and appropriate confidentiality of information. Primary objectives include development and implementation of proactive measures to prevent security problems and effective response to security problems when prevention methods are defeated.

Scope

This charter applies to all people who maintain or manage university IT resources, their supervisors and their unit administrators. It applies to all locations of those resources, whether on campus or remote locations. It applies to all SGTU and unit policies, standards and procedures, some of which are listed below. This charter is intended to help protect integrity, availability, accountability and appropriate confidentiality of SGTU IT resources. Additional standards and



Registrar
SGT University
Budhera, Gurugram

procedures may govern specific data, computers, computer systems or networks provided or operated by specific SGTU and subsidiary units.

Acceptable Use of Computing Resources

SGTU Policy for Security Management Responsibilities

SGTU Physical Security Standard

SGTU Network Security Standard

SGTU Software Security Standard

SGTU Risk Assessment Standard

SGTU Incident Response Standard

SGTUIT Training and Security Awareness Standard

SGTU Data Security Standard

Business Resumption Standard

Enforcement

Unit administrators and IT workers who fail to adhere to this charter may be subject to penalties and disciplinary action, both within and outside the university. Violations will be handled through the university disciplinary procedures applicable to the relevant Unit or IT employee. The university may suspend, block or restrict access to IT resources, IT workers, and/or Units independent of such procedures, when it reasonably appears in the best interest of the University to do so. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Definitions

SGTU Unit:

College, Department, Research Center, Institute or other administrative subdivision connected to the SGTU network.

Subsidiary Unit:


Registrar
SGT University
Budhera, Gurugram

A major unit which has a distinct and divergent mission statement from that of SGTU, and which in some cases may also be a separate legal entity, such as Shands.

Associate:

An entity external to SGTU that performs functions or activities that involve the use or disclosure of information on behalf of, or provides services to, the University.

IT resource:

Any equipment used to store, process, and display or transport digital information is an IT resource. The associated data, applications and hardware, are also IT resources.

Information Technology (IT) worker:

An individual hired by a unit to manage or maintain IT resources in that unit. IT duties must be specified in the job description.

Roles and Responsibilities

SGTU information security roles are organized in three main levels: Level 1 has responsibility for the entire university, Level 2 units are listed below, and Level 3 has responsibility for smaller units within Level 2 units. More levels may be added at the discretion of those responsible for Level 2.

SGTU IT Security Administrator (SGTU ISA)

The SGTU ISA has the responsibility to ensure implementation and management of the SGTU IT security program. The SGTU ISA has the authority to direct action as needed to protect SGTU IT resources. The SGTU ISA has the authority to enforce SGTUIT policies, standards, and procedures and to direct action related to violations. Where questions arise with respect to what constitutes a unit, the SGTU ISA has final authority.

SGTU IT Security Manager (SGTU ISM)

The SGTU ISM manages the SGTUIT security program and security team. The SGTU ISM is responsible for coordinating efforts to create and maintain

centralized SGTU IT security policies, standards, and procedures. The SGTU ISM or a designee is responsible for enterprise risk assessment, enterprise network intrusion detection, working with Level 2 Unit ISMs to resolve exposures and reduce potential exposures, the SGTU security web site, and organizing IT security training and awareness events. The SGTU ISM is responsible for maintaining only Level 2 Unit ISA and Unit ISM contact information. Level 2 Unit ISAs and ISMs are listed in the contact database maintained by Network Services.

IT duties must be specified in the job description of the SGTU ISM.

Level 2 Unit IT Security Administrator (Unit ISA)

At a minimum, security authority and responsibility must be defined at the division or college level. The highest level unit administrator is the Level 2 Unit ISA, but this authority may be delegated. IT security responsibilities and reporting structure within the unit are at the discretion of the Level 2 Unit ISA, but a structure based to the SGTU structure is recommended with security administrators and security managers designated in each sub-unit.

The Level 2 Unit ISA has the responsibility to ensure implementation and management of the unit's IT security program. They have the authority to direct action as needed to protect unit IT resources. They have the authority to enforce SGTU and unit IT policies, standards, and procedures and to direct action related to violations. Each Level 2 Unit ISA must appoint an Level 2 Unit Information Security Manager (Unit ISM). The higher level unit has the discretion to designate ISMs at subordinate unit levels, but contact information must be maintained by the Level 2 Unit ISM.

Where appropriate, IT duties must be specified in the job description of the Level 2 Unit ISA.

Level 2 Unit IT Security Managers (Unit ISM)

Level 2 Unit ISMs are responsible for managing and coordinating security efforts within that unit's organizational hierarchy. The Level 2 Unit ISM has the responsibility to advise unit administration of security implementations consistent with SGTUIT policies, standards, and procedures. While the Level 2


Registrar
SGT University
Budhera, Gurugram

Unit ISM is responsible to their unit administrative structure, they must be made known to the SGTU ISM.

To ensure professional management of SGTUIT resources, the Level 2 Unit ISM must ensure that their unit complies with SGTUIT security policies, standards, and procedures and that employee in their unit are aware of applicable laws, policies, standards, and procedures.

All units must have specific written IT security policies, standards and procedures. The Level 2 Unit ISM, in cooperation with the Level 2 Unit ISA, is responsible for the coordination of unit IT security policies, standards, and procedures. Unit security policies, standards, and procedures must be available to the SGTU ISM upon request. Units must create standards for physical access, network and host access, incident response, data security, business resumption, awareness, etc.

It is possible that ISM duties for smaller units do not require a full-time commitment and may be assigned to an existing IT position. IT duties must be specified in the job description of the Level 2 Unit ISM. The Level 2 Unit ISM must coordinate with their unit administration to ensure that all networks in their unit have adequate professional coverage, including vacation alternates. The Level 2 Unit ISM must maintain contact information for their unit IT staff and appropriate alternates. The Level 2 Unit ISM must ensure that all people who manage IT resources in their unit are appropriately trained and aware of relevant laws, and SGTU policies, standards, and procedures. The Level 2 Unit ISM must coordinate within their unit various IT security responsibilities, including but not limited to monitoring, documenting, reporting, and correcting the cause of security breaches, establishing minimum security standards for the installation and configuration of IT resources, maintaining the operating systems, reviewing account termination, ensuring secure coding, and other security functions.

The Level 2 Unit ISM must be a permanent employee with more than 50% IT related job responsibility. They must have a high school diploma or equivalent, and at least 4 years of professional IT related job experience. IT related vocational training or college course work may substitute for experience. The Level 2 Unit ISM must be a full-time employee. An FBI background check is recommended for all people who maintain or manage IT resources, but is


Registrar
SGT University
Budhera, Gurugram

required before an individual is assigned Level 2 Unit ISM duties. Existing employees not on probation at the time this charter is implemented do not require an FBI background check.

The Level 2 Unit ISM should pursue IT security related continuing education such as Information Technology Security Awareness Day.

IT workers

IT workers maintain, manage, or have responsibility for SGTU IT resources. All IT workers must be qualified to implement SGTU and respective unit IT policies, standards, and procedures appropriate to their level of job responsibility, or they must be closely supervised by someone who is. Where questions arise with respect to qualifications of IT worker candidates, the hiring authority must coordinate with the Level 2 Unit ISM and the Unit ISA

IT duties must be included in job descriptions of IT workers.

IT workers are responsible to keep informed of changes to SGTU and respective unit IT policies, standards, procedures, and other information resources.

SGTU IT Resource Categories

In terms of management and responsibility, the SGTU recognizes the following categories of IT resources: professionally managed, personally managed, and managed by business associates. These categories are described below.

Professionally Managed IT Resources

Professionally managed IT resources are maintained by IT workers in a manner consistent with SGTU IT policies, standards, and procedures. Non-IT workers should not manage SGTU IT resources. Qualified professional IT consultants may be contracted to manage or maintain unit IT resources, but must comply with SGTU and respective unit IT policies, standards, and procedures. If the unit cannot support IT workers, they should seek assistance from IT workers in another unit or contact the SGTU ISM.

Personally Managed IT Resources


Registrar
SGT University
Budhera, Gurugram

All SGTU IT resources must be managed by SGTUIT workers. The Level 2 Unit ISA can make exceptions for research or other purposes and allow non-IT workers to manage IT resources. These are referred to as personally managed IT resources. Personally managed IT resources also include personally owned devices such as laptops, computers, PDAs, and other IT equipment. Personally managed IT resources commonly connect in classrooms, at walkups, with wireless, and on the student residential network. Personally managed IT resources must meet the following requirements.

Before connecting to the SGTU Network, personally managed IT resources must connect only to designated network zones.

All personally managed IT resources connecting to unit networks must be coordinated with the Level 2 Unit ISM

The Level 2 Unit ISM must ensure that maintainers of personally managed IT equipment in their unit are aware of relevant SGTU IT security policies, standards, and procedures.

The Level 2 Unit ISM must ensure that maintainers of personally managed IT resources comply with relevant SGTU IT security policies, standards, and procedures.

IT Resources Managed by Associates

Associates that manage IT resources on the SGTU network must be informed of SGTU IT security policies and sign an agreement to comply with them. SGTU and Level 2 Unit ISMs must maintain contact information for all Associates managing IT resources on networks for which they are responsible. Requests for exceptions to this policy must be submitted in writing by the Level 2 Unit ISM to Information Technology Advisory Committee – Information Security Management (ITAC-ISM). The SGTU ISM will respond to all requests for exceptions in writing.

AUDIT AND LOGGING POLICY

Purpose

Registered
SGT University
Budhera, Gurugram

To provide accurate and comprehensive audit logs in order to detect and react to inappropriate access to, or use of, information systems or data.

Scope:

This policy applies to all Information Systems that store, process or transmit University Data.

Policy:

1. Access to Information Systems and data, as well as significant system events, must be logged by the Information System.
2. Information System audit logs must be protected from unauthorized access or modification.
3. Information System audit logs must be retained for an appropriate period of time, based on the Document Retention Schedule and business requirements. Audit logs that have exceeded this retention period should be destroyed according to SGTU document destruction policy.

Responsibilities:

1. Information System Administrators (ISAs) are responsible for developing and implementing procedures for the reporting and handling of inappropriate or unusual activity.
2. Information System Managers (ISMs) are responsible for monitoring and reviewing audit logs to identify and respond to inappropriate or unusual activity.

CONTROL OF ELECTRONIC MEDIA

Purpose

The purpose of this policy is to provide safeguards for electronic media to prevent loss of access to, or unauthorized disclosure of, University Data.

Scope:


Registrar
SGT University
Budhera, Gurugram

This policy applies to all electronic media used with university Information Systems or University Data.

Policy:

1. All electronic media must be securely erased or destroyed prior to disposal, transfer or reuse outside of the university. The University Standard for Media Sanitization must be followed.
2. Electronic media containing Restricted Data must be protected from theft, accidental loss or damage in accordance with all SGTU information security and privacy policies and standards.

Responsibilities:

1. All members of the SGTU Constituency are responsible for protecting electronic media under their use or control.
2. All members of the SGTU Constituency must promptly report loss or theft of electronic media containing Restricted Data to the SGTU Privacy Office.
3. Information Security Administrators (ISAs) are responsible for developing and implementing procedures to protect electronic media.
4. The IT Department is responsible for implementing systems and specifications to facilitate unit compliance with this policy.


IDENTITY MANAGEMENT POLICIES

Purpose

The university requires a secure and reliable method of identifying members of its community for access to electronic data resources. This requires collecting and maintaining identifying attributes, ensuring that electronic identities match the appropriate persons, and mechanisms to authenticate and authorize use of those identities.

Scope:

Registered
SGT
Budh
ity
urgra



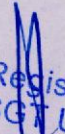
This policy applies to everyone with an identity included in the university's central identity registry, as well as individuals authorized to perform identity management (IdM) functions on behalf of the university.

Policy:

1. The university will maintain a ERP that will serve as a central store for identity and account information.
2. All identities within the central identity registry will be assigned a unique SGTU ID number. SGTU ID numbers will never be re-issued to a different identity.
3. All identities within the ERP will be assigned an Identity Assurance Profile as defined in the related Identity Assurance Profile Standard document.
4. Required attributes for each identity, depending on the Identity Assurance Profile, must be complete, accurate and current.
5. The university may participate in identity federation, whereby holders of SGTU identities can be granted access to resources hosted outside the university, and holders of Identities from federated entities can be granted access to resources hosted by the university.

Responsibilities:

1. SGTU students, employees and other enterprise workforce members must maintain accurate contact and demographic data in the SGTU ERP
2. IdM Coordinators must actively maintain complete and accurate data in the ERP in collaboration with, and on behalf of people within their scope of authority. An IdM Coordinator is a SGTU workforce member who maintains data related to a person's identification contained in the SGTU Directory for a specific unit of the SGTU enterprise. Individuals are delegated authority from the dean, director (or DDD) of the unit.
3. Primary IdM Coordinators are responsible for assuring complete and accurate identity information is in place for identity credentialed personnel within their scope of authority, and according to Identity Assurance Profile standards. A primary IdM coordinator is a SGTU workforce member who serves as the primary


Registrar
SGTU University
Budhara, Gurugram

contact for questions related to a person's identification data for a unit. They are appointed by the dean or director of the unit.

4. SGTU IdM Coordinators serving as a Registration Authority (RA) must adhere to Identity Assurance Profile standards for the applicable level of access when provisioning credentials for SGTU workers. A registration authority is an Idm Coordinator or Primary IdM Coordinator who has had additional special training to perform the credential verification functions to certify a user to meets Identity Assurance Profiles the require in person review.

IDENTITY ASSURANCE PROFILES STANDARD

Purpose:

Establish multiple levels of assurance for electronic identities, with attributes and requirements for their issuance. Multiple levels are needed to conduct the varied functions of the university, but can be handled without subjecting all users to the most rigorous levels of security.

Scope:

All electronic identities and accounts issued and maintained through the university's ERP.

Standard:

See the chart at the bottom of this document for the minimal attribute requirements for all each Identity Assurance Profile (IAP) defined in this standard.

SGTU GUEST

SGTU Guest is a short-term temporary access level, for visitors to the SGTU campus who require temporary access to minimal services. Guests are not eligible for a permanent ID and not listed in the ERP. Examples are seminar participants needing Internet access.


Registrar
SGT University
Budhera, Gurugram

IDENTITY MANAGEMENT SERVICE PROVIDER STANDARD

Purpose

To establish requirements for services that make use of the university's central identity registry to perform authentication and authorization that will ensure the security and integrity of identity information.

Scope:

Any Service Provider that uses information from the ERP to authenticate and authorize users. Examples of technologies that incorporate information from the ERP for use by Service Providers.

Standard:

1. Service Providers must never commit user passwords to persistent storage.
2. Shibboleth is the preferred authentication and authorization technology for web applications.
3. Inclusion in the central identity registry provides no assurance of a person's standing with the university. Authentication of credentials should be augmented with authorization assertions.
4. Service Providers should use appropriate authorization techniques and attribute assertions available from the SGTU identity provider to verify that users are eligible to access the provided resources. Examples include checking level of assurance, affiliations, granted roles or group memberships.
5. Service Providers should not use any login screen that is not provided by the SGTU. Exceptions to this may be granted after review of a Service Providers specific situation. Requests for exceptions can be made to the Identity & Access Management Office.

INTERNET PROTOCOL ADDRESS ASSIGNMENT POLICY

INTERNET PROTOCOL ADDRESS ASSIGNMENT STANDARD

Purpose


Registrar
SGT University
Budhera, Gurugram

The SGTU computer network is based on the Internet Protocol (IP). IP networks function using pre-assigned addresses and their misuse can disrupt network functionality. Further, the SGTU is assigned a limited number of public IP addresses, which are used to communicate with the Internet. The allocation of these addresses must be managed to optimize the SGTU's ability to provide services to users on the Internet, and to access resources available on the Internet.

Scope

This policy applies to all uses of IP addresses on the SGTU network.

Policy

1. All IP addresses used on the SGTU network will be assigned by IT Department.
2. All IP addresses used on the SGTU network must be registered with Infrastructure and Communication Technology (ICT).

Responsibilities

1. IT Department will establish standards for assignment and use of IP addresses at the SGTU.
2. IT Department is responsible for implementing systems and specifications to facilitate unit compliance with this policy.
3. SGTU IT will establish an IP address utilization plan and allocate IP addresses per the plan.
4. SGTU IT is responsible for appointing Network Contacts to manage their IP address space.
5. SGTU IT is responsible for insuring that all existing uses of IP addresses comply with all relevant SGTU Policies and Standards.

WIRELESS NETWORK POLICY

All organizations with wireless LANs already deployed shall contact SGTU IT for coordination. Ideally SGTU IT can, over time, work with all existing WLAN installations to incorporate them into the campus system.

Registrar
SGT University
Budhera, Gurugram

Organizations who are contemplating deploying WLANs must contact SGTU IT to assist in the configuration and deployment of their local wireless system and to incorporate it into the campus wide system. Per the SGTU Acceptable Use Policy, individuals shall not implement their own network infrastructure. This includes, but is not limited to, Wireless Access Points (WAPs), routers, and hubs. If wireless devices that have not been installed in cooperation with SGTU IT are discovered attached to the network, a reasonable attempt will be made to contact the owner prior to disabling the network port to which it is attached. WAPs or network devices causing denial of service will be shut down immediately.

If it is not possible to integrate organizational WLANs into the campus system, or if a private WLAN is agreed upon, the following requirements shall be followed in the deployment of the WAPs:

1. The Service Set Identifier (SSID) of the WAP shall NOT be set to 'SGTU'. This is the SSID used by the University system. Use of this SSID near the campus wireless system could prevent users from accessing the campus system.
2. The broadcast SSID feature of the WAP shall be disabled and the transmit power of the AP should be lowered, if possible, to only as high as needed to cover the desired area.

WLANs shall not be used in place of wired connections. WLANs shall only be used to provide service to mobile devices. SGTU IT should be contacted if there is a question about the viability of a WLAN installation.

Current WLAN technologies generally use unlicensed radio frequency ranges. Because these are unlicensed frequency bands, many other devices also operate in these bands, including other types of WLAN equipment. Use of these items on the University campus could negatively impact the SGTU wireless network. The use of these devices is not prohibited but, if a conflict is discovered, the department or individual using the device will work with the applicable LAN manager to determine an appropriate solution. Reasonable effort will be made to provide an alternative or a remedy to the problem but if the situation is irresolvable the University reserves the right to remove the offending device from service. If the device in question serves a critical need it may be given priority


Registrar
SGT University
Budhera, Gurugram

over the WLAN installation with the understanding that this may prevent WLAN use in the area.

ADVERTISING ON UNIVERSITY WEBSITE

ADVERTISING ON UNIVERSITY WEBSITE

DOMAIN NAME POLICY

INTERNET PRIVACY POLICY

RECOGNIZING CORPORATE SUPPORTERS ON THE WEB

WEB ADMINISTRATION POLICIES AND STANDARDS

WEB IDENTITY AND GRAPHICS STANDARDS

RELATED STANDARDS & DOCUMENTS

Purpose

This policy has been implemented because of the numerous business, legal and policy issues that arise in connection with the sale of advertising on university and unit web space.

Advertising consists of techniques and practices used to bring products, services, opinions, or causes to public notice for the purpose of persuading the public to respond in a certain way toward what is advertised. Advertising differs from the recognition of university supporters in that it may contain promotional or other information about a person or entity's product, services or facilities that goes beyond mere acknowledgment of support to the University. This policy does not address treatment of university supporters, which is discussed in the University's policy for Recognizing Supporters on the University & Unit Web Space.

Scope

This policy covers all web sites and web pages hosted by or on the behalf of the SGTU and all of its constituent units.


Registrar
SGT University
Budhera, Gurugram

Policy

Only the following units of the university may place advertising on their web pages:

University Athletic Association, Inc.

SGTU Foundation, Inc.

SGTU Alumni Association, Inc.

Business Services Division

College of Journalism and Communications

Responsibilities

1. The President or designee(s) may approve additional units that may place advertising on the unit's web pages
2. The University's Office of General Counsel or the SGTU Foundation's legal staff will review all contracts for advertising

DOMAIN NAME POLICY

Purpose

The Domain Name System (DNS) is an Internet-wide distributed database of names translating Internet Protocol (IP) addresses into easily memorable names. Domain names are part of the identity of the university and communicate the university's image and reputation to the public. Consistent domain usage may also be a tool for users to better locate services; thus, domains should be assigned in an easily recognizable and predictable structure. To ensure that domain names are assigned and used appropriately and in alignment with institutional goals, the university has established a policy for governing third level domain name registrations. Examples of third-level domains names would be in the form of unit name. sgtuniversity.ac.in



Registrar
SGT University
Budhera, Gurugram

Scope

This policy covers all academic and administrative units, university affiliates, and academic and administrative staff seeking to register a domain name.

Policy


1. Requests for all third-level domain names must be made by a college or administrative division that serves the entire university community and the requested third-level domain name must be approved before use.
2. All official university web sites shall use domain names within the sgtuniversity.ac.in namespace.
3. Requested third-level domain names must meet the following requirements in order to be approved:
 1. The requested name should accurately describe the activity or program to which it refers and be easily recognized as word(s) or abbreviation(s).
 2. The requested name represents the unit or service used by the entire university community.
 3. The unit must expect to provide these services on an ongoing basis.
 4. Domain names shall not contain "SGTU" in addition to sgtuniversity.ac.in

Responsibilities

1. IT Department or designee, approves requests for third-level domain names.

Commitment to Privacy

The SGTU values individuals' privacy and actively seeks to preserve the privacy rights of those who share information with us. Your trust is important to us and we believe you have the right to know how information submitted through a university Web site is handled.



Registrar
SGT University
Budhéra, Gurugram

We provide the following privacy notice to define SGTU's Web-based information policies and practices, and to assist you in protecting your privacy.

Privacy Notice

The following information explains the Internet privacy policy and practices the University has adopted for its official Web sites. However, in legal terms, it shall not be construed as a contractual promise, and the University reserves the right to amend it at any time without notice. Privacy and public records obligations of the University are governed by applicable laws.

Site Definitions

University Web space includes hundreds of sites with varying levels of University involvement and commitment as outlined below.

Official University Web Sites

Except as noted, the information in this privacy notice applies to all official SGTU Web sites, which are defined as the Web pages of university colleges, schools, departments, divisions or other units and any other sites specifically designated as official by a vice chancellor, dean, department head or director. Official pages are generally recognizable by a standard page header and/or footer carrying the University logo, contact information and reference to this privacy statement.

Unofficial Web Sites

Within the SGTU domain – signified by the address "sgtuniversity.ac.in" or within the range of Internet protocol addresses assigned to the SGTU– you may find Web sites over which the University has no editorial responsibility or control. Such sites are considered unofficial and include, but are not limited to, the Web pages of individual faculty members or students and the Web pages of student organizations and other entities not formally a part of the University. While SGTU encourages compliance with this Web Privacy Statement at such sites, in order to better understand the policies and practices under which they operate, please consult the privacy statements of individual sites or seek information directly from the persons responsible for those sites.


Registrar
SGT University
Budhera, Gurugram

The Web Privacy Statement speaks generally to the information collected by or submitted to official SGTU Web sites. Still the amount and type of information collected may vary somewhat from site to site. Therefore, in addition to this general explanation of policy and practice, the University encourages colleges, schools, departments, divisions and other units contributing to its official Web pages to post, as necessary, more specific approved privacy notices pertaining to the collection and use of any personal information associated exclusively with those pages. Thus it is wise for users to read page-specific notices to better understand the privacy policies and practices applicable to a particular site.

The Information We Collect

When you access official SGTU Web pages, certain client information and essential and nonessential technical information (collectively referred to as access information) listed below is automatically collected. No other information is collected through our official Web sites except when you deliberately send it to us (for example, by clicking a link to send us an e-mail). Examples of the information you might choose to send us are listed below as "optional information."

Access Information (automatically collected)

Client information: the Internet domain and Internet address of the computer you are using.

Essential technical information: identification of the page or service you are requesting, type of browser and operating system you are using; and the date and time of access.

Nonessential technical information: the Internet address of the Web site from which you linked directly to our Web site, and the "cookie information" used to direct and tailor information based on your entry path to the site.

Optional information (deliberately sent)

E-mail: your name, e-mail address, and the content of your e-mail.

Online forms: all the data you choose to fill in or confirm. This may include credit or debit card information if you are ordering a product or making a payment, as


Registrar
SGTU University
Budhera, Gurugram

well as information about other people if you are providing it for delivery purposes, etc. See below for more specific information about children's online activities.

The Way We Use Information

As a general rule, SGTU does not track individual visitor profiles. We do, however, analyze aggregate traffic/access information for resource management and site planning purposes. SGTU reserves the right to use log detail to investigate resource management or security concerns.

Access Information

Client information is used to route the requested Web page to your computer for viewing. In theory, the requested Web page and the routing information could be discerned by other entities involved in transmitting the requested page to you. We do not control the privacy practices of those entities.

We may keep client information from our systems indefinitely after the Web page is transmitted, but we do not cross-reference it to the individuals who browse our Web site. However, on rare occasions when a "hacker" attempts to breach computer security, logs of access information are retained to permit a security investigation. In such cases the logs may be further analyzed or forwarded together with any other relevant information in our possession to law enforcement agencies.

Under the Florida Public Records Laws, certain records in our possession are subject to inspection by or disclosure to members of the public. As indicated above, client information retained after transmission of the requested Web page will be available for inspection.

Essential and nonessential technical information lets us respond to your request in an appropriate format [or in a personalized manner] and helps us plan Web site improvements. To expedite this process, some official SGTU Web sites use "cookies." Usually a cookie enables the university Web site to tailor what you see according to the way you entered the site (i.e., if you entered by pushing a button identifying yourself as a student, your subsequent views of information might be tailored for student audiences).


Registrar
SGT University
Budhera, Gurugram

We also use non-identifying and aggregate information to better design our Web site. For example, we may determine that X number of individuals visited a certain area on our Web site, or that Y number of men and Z number of women filled out a particular registration form. But we do not disclose information that could identify those specific individuals.

Optional Information:

Optional information enables us to provide services or information tailored more specifically to your needs, to forward your message or inquiry to another entity that is better able to do so, and to plan Web site improvements.


We use the information you provide about yourself or about someone else when placing a request for service only to complete that order or request. We do not share this information with outside parties, except to the extent necessary to complete that order or request.

We generally use return e-mail addresses only to answer the e-mail we receive. Such addresses are generally not used for any other purpose and by university and state policy are not shared with outside parties.

Finally, we never use or share the personally identifiable information provided to us online in ways unrelated to the purpose described without a clear notice on the particular site and without also providing you an opportunity to opt-out or otherwise prohibit such unrelated uses.

Public Records Notice: Providing Information is Your Choice

There is no legal requirement for you to provide any information at our Web site. However, our Web site will not work without routing information and the essential technical information. Failure of your browser to provide nonessential technical information will not prevent your use of our Web site but may prevent certain features from working. For any optional information that is requested at the Web site, failure to provide the requested information will mean that the particular feature or service associated with that part of the Web page may not be available to you.



Registrar
SGT University
Budhera, Gurugram

Our Commitment To Data Security

The SGTU is dedicated to preventing unauthorized data access, maintaining data accuracy, and ensuring the appropriate use of information. We strive to put in place appropriate physical, electronic, and managerial safeguards to secure the information we collect online. These security practices are consistent with the policies of the university and with the laws and regulatory practices of the State of Florida.

RECOGNIZING CORPORATE SUPPORTERS ON THE WEB

Purpose

The purpose of this policy is to direct units on how they may appropriately recognize supporters on university and unit web space without overly commercializing the University and unit home pages.

These guidelines do not address advertising on university web space, which is governed by the University's Policy for Advertising on University & Unit Web Space. Recognition of corporate support differs from advertising in that it only acknowledges support to the University; it does not contain promotional or other information about a person or entity's product, services or facilities.

Scope

This policy covers all web sites and web pages hosted by or on the behalf of the SGTU and all of its constituent units.


Policy

The University and individual units may recognize significant supporters on their secondary web pages. Vendors that provide goods or services to the University or individual units do not qualify for recognition as university supporters solely by virtue of their contract.

Responsibilities


Registrar
SGT University
Budhera, Gurugram

-
1. The President or their designee will determine eligibility for designation as a university supporter, based on whether the supporter provides significant support to the university-wide mission.
 2. The head unit administrator or designee will determine eligibility for designation as a unit supporter, based on whether the supporter provides significant support to the unit.
 3. SGTU Foundation representatives will review all proposed university or unit supporters prior to inclusion on a web page. Units interested in recognizing unit supporters should work with their SGTU Foundation representatives.
 4. The President or designee, or in the case of unit pages, the head unit administrator or their designee will designate the period of time for which to recognize the university or unit supporter.



Registrar
SGT University
Budhera, Gurugram