B.S. Abdur Rahman Crescent Institute of Science & Technology
Deemed to be University u/s 3 of the UGC Act, 1956
GST Road, Vandalur, Chennai 600 048

IT Policy

V1.0

B.S. Abdur Rahman Crescent Institute of Science & Technology
Deemed to be University u/s 3 of the UGC Act, 1956
GST Road, Vandalur, Chennai 600 048

Prepared By	Reviewed By	Approved By
Dr. Sharmila Sankar Dr. Latha Tamilselvan Dr. W. Aisha Banu Dr. B. Vijayalakshmi Dr. N. Rajendran G. Sureshkumar	Dr. M.S. Haji Sheik Mohammed	Dr. A. Azad
IT & Software Policy Committee	Dean – Academic Affairs	Registrar

B.S. Abdur Rahman Crescent Institute of Science & Technology
Deemed to be University u/s 3 of the UGC Act, 1956
GST Road, Vandalur, Chennai 600 048

Table of Contents

1. IT Software Policy---------- 4

2. IT Network Policy---------- 9

3. IT Hardware Policy----------15

4. IT Security Policy----------24

5. IT Website Policy----------45

6. IT Maintenance Policy----------51

B.S. Abdur Rahman Crescent Institute of Science & Technology
Deemed to be University u/s 3 of the UGC Act, 1956
GST Road, Vandalur, Chennai 600 048

IT Software Policy

Overview

In modern world the usage of Information Technology (IT) Software is unavoidable and for institutions like B S Abdur Rahman Crescent Institute of Science & Technology (BSACIST) the need is more to keep up with technology in order to have the students trained. In order to have this in place a Policy for Software Usage, purchase, installation, maintenance and Management is mandatory

Purpose

The purpose of this document is to create a Policy for Usage, purchase, installation, maintenance and Management of authorized Software in our institution. This will help in minimizing the need of repeated follow-up or avoiding un-authorized Software in our campus thereby having a standard operating environment with a pre-defined Service Level Agreement(SLA). This also helps in easier management of software's.

Scope

This policy applies to all members of the institution including students, teaching staff, non-teaching staff, visiting faculties, vendors and contractors. This policy covers the Usage, Purchase, installation, maintenance and Management of the IT Software.

Software Policy

The purpose of the BSACIST Software Policy is to ensure that BSACIST employees are properly trained on appropriate procedures for using the software's in a legitimate manner. As a primary objective of the institution, it is encouraged to use Open Source Software across the institution. Also, this policy discourages any usage of illegal non-licensed or un-authorized Open Source Software in the IT assets of BSACIST by all the people directly or indirectly related to this organization.

Software Usage Terms

- All members are not allowed to install software directly in the institution IT assets.

- Faculty, Lab's and Support departments by default needs to use Open Source Software
- Only as an exception, licensed software's with proper justification and approvals will be taken for consideration.
- All requests for software need to be pre-approved by the department& institution head and sent to Data centre team.
- If the approved software is open source, freeware or demo software then it will be verified and approved by Director – Data centre and installed by Data centre Team members. Usage of this software needs to be within the terms and conditions bound by software and any violation will be subject to disciplinary action.
- If the approved software is supplied by a licensed Original Equipment Manufacturer(OEM), then it will be approved by Director – Data centre and procured as per the standard process and will be installed by Data centre Team members and the license will be in the name of BSACIST
- Duplication of license is strictly prohibited among the IT assets in BSACIST.
- If Software is eligible for home usage, then it should be pre-approved by the Department Head / Director Data centre before usage. The usage of this is limited to Official purpose and should be revoked once the employee leaves BSACIST
- If Software is eligible for free usage in education institutions, then it will be verified by the Department Head / Director Data centre before proceeding with the installations.
- In order to maximize the usage of the licensed Software, they can be purchased as Stationed based licenses or common user based licenses. In such scenarios the departments are liable to keep a record of users who uses the software's in this method.
- Data centre Team keeps a record of the software licenses procured, distribution list, serial numbers, receipts and invoices, Software licensing terms along with the end date of agreement
- Original Software DVD procured will be stored in Data centre.
- Any Transfer of licenses between the departments needs to be approved by Department Heads / Deans along with Director- Data centre for initiation of transfer.

- Un-installation of licensed software will be done with necessary approvals by Data centre team.
- Any obsolete software that needs to be disposed / written off will be approved by Director-Data centre and Finance before disposal.
- Any personal Software installation within the institution is strictly prohibited.
- Renewal or extension for the usage of Software's procured has to be pre-approved by the department& institution head and sent to Data centre team. Data centre team will validate and will supply with necessary quotes for Director's approval. Based on the approval from Management the Software will be renewed or extended for the usage in IT assets.
- All Software's approved and used inside the campus needs to abide by the usage terms and conditions and any violation found will result in software revocation.
- All IT systems should be protected by Antivirus Software.
- Network administration tools are not allowed without consent of Director –Data centre. This includes but not limited to Network monitors, sniffers, port scanners and SNMP tools.
- Reconciliation of unused software should be done in a periodic time frame.
- Requesters of such unused software are accountable for the expenses incurred.

Procedure Compliance

- The Data centre Team will conduct periodic verification via physical verification, ITAM tool reports, internal and external audits.
- The Data centre team has the rights to monitor the BSACIST software's usage on the organization's IT assets whether in campus or working on a remote location.
- Leaving staffs should release the IT Software's and handing over any Media with the help of Data centre team before the final clearance from the organization.
- Any Exceptions, needs to be obtained in prior accordance with the Data centre Team.
- Any Non-Compliance found to be violated as per this policy will be subject to disciplinary action.

Keywords and Abbreviations

KEYWORD	DEFINITION
IT	Information Technology
OEM	Original Equipment Manufacturer
Software	General term used for Software including Operating Systems, Office usage Software, LAB Software, Open Source Software etc.
Hardware	General term used for hardware including Routers, Switches, Firewalls, Servers, Storage, Desktops, Laptop, Printers and Scanners
Installation	DVD, Download or Direct Installation via Internet
SLA	Service Level Agreement
ITAM	IT Asset Management
DVD	Digital Versatile Disc
SNMP	Simple Network Management Protocol

Contact Information

For all requests, reach out to Data centre Team and for all approvals and escalations please reach out Director – Data centre.

Revision History

Date of Change	Version Number	Section	Done By	Summary of Change
22-12-2020	V1	All	Data centre Team & IT SW Policy committee	Creation of IT Software Policy

B.S. Abdur Rahman Crescent Institute of Science & Technology
Deemed to be University u/s 3 of the UGC Act, 1956
GST Road, Vandalur, Chennai 600 048

IT Network Policy

Overview

Today's world has shrunk a lot due to growth of the modern IT Network. IT Network is huge, vast in options and changes daily due to innovation. In order to maintain a uniformity and standardization we need to have a Policy in place for network usage, purchase, installation, maintenance and management.

Purpose

The purpose of this document is to create a Policy for usage, purchase, installation, maintenance and management of authorized Network devices and bandwidth in our institution. This will help in avoiding non-standardized Network devices in our campus thereby having a standard operating environment with a pre-defined SLA.

Scope

This policy applies to all members of the institution including students, teaching staff, non-teaching staff, visiting faculties, vendors and contractors. This policy covers the Usage, Purchase, installation, maintenance and Management of the ICT Network.

Network Policy

The purpose of the Crescent Network Policy is to ensure that Crescent employees are properly trained on appropriate procedures for using the Network and its resources in a legitimate manner for a secured campus network. This policy also discourages unauthorized users and any usage of non standardized Network devices and bandwidth service providers in our campus thereby reducing the security risk posed by our Network.

Network Usage Terms

1. All members are not allowed to install Network devices directly in the institution
2. All requests for Network and bandwidth needs to be pre-approved by the Department Heads /Deans before submitting the requests to Data centre team
3. If the approved device is supplied by a licensed OEM, then it will be approved by Director – Data centre and procured as per the standard procedure and will be

installed by Data centre Team members and the device will be in the name of Crescent

4. If device is eligible for home usage then it should be pre-approved by the Department Head / Director Data centre before usage. The usage of this is limited to Official usage and should be revoked once the employee leaves Crescent
5. Data centre Team keeps a record of the Network devices procured, distribution list, serial numbers, receipts and invoices, licensing terms along with the end date of agreement
6. Original Installation / Serial number Software DVD procured will be stored in Data centre.
7. Any Transfer of Network devices between the departments needs to be approved by Department Heads / Deans along with Director- Data centre for initiation of transfer.
8. Un-installation of Network devices will be done with necessary approvals by Data centre team.
9. Any obsolete network device that needs to be disposed / written off will be approved by Director-Data centre and Finance before disposal.
10. Any personal network device usage within the institution is strictly prohibited.
11. Renewal or extension for the usage of network / bandwidth has to be pre-approved by the department heads and sent to Data centre team. Data centre team will validate and will supply with necessary quotes for Director's approval. Based on the approval from Management the network / bandwidth will be renewed or extended for the usage in our campus.
12. All Network devices and bandwidth approved and used inside the campus needs to abide by the usage terms and conditions and any violation found will result in device revocation.
13. Logins into the Crescent Network devices should be welcomed with a banner stating the usage terms for the users to avoid any third party accidental logins.
14. High Availability to be implemented wherever possible for network devices, login servers and ICT Bandwidth providers to overcome disaster scenarios.

Wired Network

1. Any Wired device that is requested needs to be from a standard OEM vendor in the industry who has reputed standard and support model
2. Usage of Layer 2 and Layer 3 devices wherever necessary will be evaluated and recommended by Data centre Team
3. Firewalls whether Software or Hardware based will be evaluated and procured in par with Industry standards to compete with the modern world
4. Latest Patches needs to be upgraded to the device as per recommendation from Data centre Team to avoid instability of devices and improves the security

Wireless Network

1. Wireless devices needs to be standardized within couple of models across the campus
2. Cross compatibility between these should be ensured for authentication
3. Controllers should be used authenticate the Access points
4. Access points need to be positioned in strategic points across campus with the use of heat mapping technology
5. Rogue access points should be blocked based on MAC ID's or other possible ways
6. Latest Patches needs to be upgraded to the device as per recommendation from Data centre Team to avoid instability of devices and improves the security

Access Policies

1. User names should be unique in nature along with strict enforcement for complex passwords
2. Authorization server can be used to authorize the user's logging in and based on that profiles can be allowed
3. Multiple profiles has to be used such as read only, read – write some items and admin user
4. Failure to login into the network device within 3 attempts should be blocked and the user ID is locked to prevent misuse

Procedure Compliance

The Data centre Team will conduct periodic verification via physical verification, ITAM tool reports, internal and external audits.

The Data centre team has the rights to monitor the Crescent Network usage on the organization's ICT assets whether in campus or working on a remote location.

Leaving staffs should release the ICT Networking devices and handing over any Media with the help of Data centre team before the final clearance from the organization.

Any Exceptions, needs to be obtained in prior accordance with the Data centre Team.

Any Non-Compliance found to be violated as per this policy will be subject to disciplinary action.

Keywords and Abbreviations

KEYWORD	DEFINITION
IT	Information Technology
PO	Purchase Order
SOP	Standard Operating Procedure
ICT	Information and Communications Technology
OEM	Original Equipment Manufacturer
Software	General term used for Software including Operating Systems, Office usage Software, LAB Software, Open Source Software etc.
Hardware	General term used for hardware including Routers, Switches, Firewalls, Servers, Storage, Desktops, Laptop, Printers and Scanners
Installation	DVD, Download or Direct Installation via Internet
SLA	Service Level Agreement

Contact Information

For all requests, reach out to Data centre Team and for all approvals and escalations please reach out Director – Data centre.

Revision History

Date of Change	Version Number	Section	Done By	Summary of Change
22-12-2020	V1	All	Data centre Team& IT SW Policy committee	Creation of ICT Network Policy

B.S. Abdur Rahman Crescent Institute of Science & Technology
Deemed to be University u/s 3 of the UGC Act, 1956
GST Road, Vandalur, Chennai 600 048

IT Hardware Policy

Hardware Access Policy - General

Please Read the following B S Abdur Rahman Crescent Institute of Science and technology (BSACIST), 'Hardware Usage Policy', CAREFULLY before accepting/rejecting the policy.

People, who use the ONLINE version for Hardware Policy Acceptance, need not sign the hardcopy version.

Whom this Document Concerns: All Users of IT hardware infrastructure (Computers and the Network) at BSACIST.

Reason for Policy: This policy outlines the responsible use of the Information Technology Infrastructure at BSACIST.

Overview

The B S Abdur Rahman Crescent Institute of Science and technology (BSACIST) is committed to fair allocation of Institute's resources, and the provision of a working environment of needless disruption. To advance these goals, the Institute has adopted policies on hardware facility usage.

In consideration with the technological advancements, from 1G, 2G to its higher level, the growth of the modern Information Technology (IT) Network incorporates the latest hardwares. It brings huge, vast in options and changes in the IC topology or end devices. In order to maintain uniformity, standardization and to keep the students trained with technology, needs a Policy for Hardware Usage, purchase, installation, maintenance and Management.

Purpose

The purpose of this policy is to secure and protect the Hardware assets in association to IC owned by B S A Crescent Institute of Science and Technology. The institute provides computer devices, networks, and other electronic communication systems to meet missions, goals, and initiatives. Institution grants access to these resources as a privilege and must

manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that hardware of IC infrastructure must satisfy the standards, while connected to the institute network. Only the specific hardware devices that meet the standards specified in this policy or are granted an exception by the IT team are approved for connectivity to the institution network.

Scope

All employees, contractors, consultants, temporary and other workers at BSACIST, including all personnel affiliated with third parties who maintain a hardware device on behalf of BSACIST must adhere to this policy.

This policy applies to all hardware infrastructure devices that connect to the institution IC system or reside on the campus site that provides RF/Optical communication connectivity to the endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of electronic communication device capable of transmitting IC data.

To establish wide strategies and responsibilities for protecting the Confidentiality, Integrity, and availability of the information assets that are accessed, created, managed, and/or controlled by the BSACIST.

All hardwares adopted to establish a IC infrastructure by B S A Crescent Institute of Science and Technology, not be affected in any case.

Hardware Policy

Statement of Policy: All users of BSACIST will be subject to the following **Acceptable Use Policy**

[Content] I shall be responsible for all use of this network. In case I own a computer and decide to connect it to BSACIST network, I will be solely responsible for all the content on it (examples: all files/data, software, Detachable memory device, Connectivity). This provision will also apply to any computer or device for which I am responsible, and is included in the

meaning of "my computer". In case I do not own a computer but am provided IC system by BSACIST, I will be held responsible for the content stored in the designated workspace allotted to me (examples: Detachable memory device, software, file storage area, web pages, stored/archived emails, on Data Centre, Computer Centre or Department machines).

[Network] I will be held responsible for all the network traffic generated by "my computer" and its associated hardware. I understand that network capacity is a limited, shared resource. I agree that physically tampering with network connections/equipments, sending disruptive signals, or making EXCESSIVE USE of network resources is strictly prohibited. Repeated offenses of this type could result in permanent disconnection of network services. I shall not share the network connection beyond my own use and will not act as a forwarder/ masquerader for anyone else.

[Academic Use] I understand that the hardware associated with the IC system at BSACIST is for academic use and I shall not use it for any commercial purpose or to host data services for other people or groups. Also, I shall not host or broadcast information that might harm others or may be otherwise considered objectionable or illegal as per Indian law.

[Identity] I shall not attempt to deceive others about my identity in electronic communications or network traffic. I will also not use BSACIST hardware associated with the IC system resources to threaten, intimidate, or harass others.

[Privacy] I will not intrude on privacy of anyone. In particular I will not try to access computers (hacking), accounts, files, or information belonging to others without their knowledge and explicit consent.

[Monitoring] I understand that the hardware associated with the IC system resources provided to me are subject to monitoring, with cause, as determined through consultation with the BSACIST administration, when applicable. The monitoring may include aggregate bandwidth usage to effectively manage limited IC system resources as well as monitoring traffic content in response to a legal or law enforcement request to do so. I authorize BSACIST administration to perform network vulnerability and port scans on my systems, hard ware, as needed, for protecting the overall integrity and efficiency of BSACIST network.

[Viruses] I shall maintain my computer and the associated hard ware on this network with current virus detection software and current updates of my operating system, and I shall attempt to keep my computer free from viruses, worms, Trojans, and other similar programs.

[Software Usage and File Sharing] I shall not use any device to engage in any form of unlicensed software storage/usage and illegal file sharing (examples: copyrighted material, obscene material).

[Library e-resources] Electronic resources such as e-journals, e-books, databases, etc. made available by the Central Library, BSACIST are for academic use. These resources can be searched, browsed, and material may be downloaded and printed as single copies of articles as is done in the case of printed library material. Downloading or printing of a complete book or an entire issue or a volume of one or more journals (called systematic downloading) is strictly prohibited. Use of hard ware, robots, spiders or intelligent agents to access, search and/or systematically download from the e-resources is also prohibited. Any violation of this policy will result in penal action as per the rules and regulations of the Institute. I am aware that Systematic downloading will result in the publisher blocking the entire community of users at BSACIST from accessing these resources.

[Security] I understand that I will not take any steps that endanger the security of the BSACIST IT infrastructure. Specifically, I will not attempt to bypass firewalls and access rules in place. This includes not setting up servers of any kind (examples: web, mail, proxy) that are visible to the world outside the BSACIST campus. In critical situations, BSACIST authorities reserve the right to disconnect any device or disable any account if it believed that either is involved in compromising the information security of BSACIST.

[Penalties] I understand that any use of IT infrastructure at BSACIST that constitutes a violation of BSACIST Regulations could result in initiation of administrative or disciplinary procedures.

[Standards] I understand all hardwares that reside at the institute site and connect to the institute IC system, or provide access to information classified as Confidential, or above must:

- Abide by the standards specified in the Information Communication Standard (Device Data Sheet). Any deviation from these standards must be approved prior to purchase.

- Be installed, supported, and maintained by an approved support team.
- Use institute approved authentication protocols and infrastructure.
- Use institute approved standard devices and equipments.
- Ensure the compatibility of interconnecting device in all aspects.
- Maintain a record for the hardware implementation over a period to be registered and tracked.
- Not interfere with the deployments maintained by the institute.
- All hardware devices acquired for or on behalf of the BSACIST or developed by BSACIST employees or contract personnel on behalf of BSACIST is and shall be deemed BSACIST property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.
- Data Centre (DC) is responsible for procurement, installation, configuration of all IT system equipments (i.e. computers, add on hard ware, Plug-ins, printers, network switches, etc) in the administrative sections at BSACIST to ensure that all equipment conforms to the hardware standards and is purchased at the best possible price.
- DC will act as a decision making body as far as the hardware systems
- No outside equipment/ hardware may be plugged into the BSACIST's network without the permission of the respective incharge and Director Data Centre.
- Policies and procedures governed by the IT and software Handbook to be followed by everyone at all times, deviation in this may result in disciplinary action, and may be reported to the law enforcement.
- All the hard ware's and plugins to be properly oriented as per the specific data sheets only.
- All spare hardware shall be stored in a cabinet or must be kept in approved Encapsulations/containers. Containers must be sealed, stacked neatly and cannot impede ingress/egress or cooling.
- Remote Hands on service requests may be denied at BSACIST campus

- Be identified as noncompliant with BSACIST Data Centre Policies regarding refuse and combustible materials.
- “Un-authenticated access of operating the equipment/hardware inside the BSACIST is strictly prohibited.
- You must have explicit permission to access or configure the device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."
- If the BSACIST network machines, “misbehaves” and causes problems for any other department or the entire campus, or disrupts services, DC will notify the concerned Section Head and disconnect the particular machine (or even the whole administrative section depending on the severity of the problem) from the core network until the problem is fixed satisfactorily.
- Computers in the administrative sections are meant for fulfilling the office automation tasks in BSACIST administration. Their use for personal entertainment/business activities is strictly prohibited.
- Policy is not intended to, and does not, grant users any contractual rights.

Policy Compliance

Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the IT team in advance.

Non-Compliance

Confirmed violations of this policy will result in consequences commensurate with the offense, up to and including termination of employment, appointment, student status, or other relationships with the institution. An employee/student found to have violated this policy may be subject to disciplinary action, up to and including termination of employment/study.

Related Standards, Policies and Processes

Specifications of individual hardware are to be strictly adhered as mentioned by specific manufacturer data sheet. Deviations in this to be justified, if not, it may result in disciplinary action, and may be reported to law enforcement.

Definitions and Terms

Hardware (H/W), in the context of IT and Software technology, refers to the physical elements that make up a computer or electronic system and everything else involved that is physically tangible. Typically, the B S Abdur Rahman Crescent Institute of Science and Technology – BSACIST - hardware includes:

Core computing equipment: Computer/machine that manipulates data according to a set of inputs and control signals

Network equipment: electronic devices which are required for communication and interaction between devices on a computer network. Specifically, they mediate data transmission in a computer network.

Storage resources: are the collective methods and technologies that capture and retain digital information on electromagnetic, optical or silicon-based storage media

Power and cooling infrastructure: Backup power consists of one or more uninterruptible power supplies (UPS), battery banks, and/or diesel / gas turbine generators with sufficient cooling arrangements for the continuous operation of IC during electric supply failures.

Input/output devices: Add on systems associated with the computing machines, to feed and get the processed information

Keywords and Abbreviations

KEYWORD	DEFINITION
BSACIST	B S Abdur Rahman Crescent Institute of Science and Technology
IT	Information Technology
IC	Information and Communications
DC	Data Centre
Software	General term used for Software including Operating Systems, Office usage Software, LAB Software, Open Source Software etc.
H/W	Represents Hardware, such as Routers, Switches, Firewalls, Servers, Storage, Desktops, Laptop, Printers, Scanners, UPS, Batteries, Wired interconnections, wireless interconnections, Powered Generators and associated cooling Systems
Device Data Sheet	Datasheet is created by the manufacturer describing the specific characteristics, with further information on the connectivity of the devices

Contact Information

- For all requests - reach out to Data centre Team and
- For all approvals and escalations please reach out Director – Data centre.

Revision History

Date of Change	Version Number	Section	Done By	Summary of Change
22-12-2020	V1	All	Data centre Team & IT SW Policy committee	Creation of IT Software Policy

B.S. Abdur Rahman Crescent Institute of Science & Technology
Deemed to be University u/s 3 of the UGC Act, 1956
GST Road, Vandalur, Chennai 600 048

IT Security Policy

1. Policies on the Use of Computers and Network Facility

1. Overview

The B S Abdur Rahman Crescent Institute of Science and technology is committed to fair allocation of Institute's resources and the provision of a working environment free of needless disruption. To advance these goals, the Institute has adopted policies on computer and Network facility usage.

2. Objective

To prohibit certain unacceptable uses of the Institute's computers and network facilities.

3. Scope

This policy covers all computers owned or administered by any part of The B S Abdur Rahman Crescent Institute of Science and technology or connected to the Institute's communication facilities, including departmental computers and personally owned computers, and also the University's computer network facilities accessed by anyone from anywhere.

4. Policy

1. No one shall use Institute's computer or network facility without proper authorization. No one shall assist in, encourage, or conceal from authorities any unauthorized use, or attempt at unauthorized use, of any of the Institute's computers or network facilities.
2. No one shall knowingly endanger the security of any Institute's computer or network facility, nor willfully interfere with others' authorized computer usage.
3. No one shall use the Institute's communication facilities to attempt unauthorized use, nor to interfere with others' legitimate use, of any computer or network facility anywhere.
4. No one shall connect any computer to any of the Institute's networks unless it meets technical and security standards set by the Institute administration.
5. Allusersshallsharecomputingresourcesinaccordancewithpoliciessetforthecomputers involved, giving priority to more important work and cooperating fully with the other users of the same equipment.
6. No one without specific authorization shall use Institute's computer or network facility for non- Institute business.
7. No one shall give any password for Institute's computer or network facility to any unauthorized person, nor obtain any other person's password by any unauthorized means whatsoever. No one except the system administrator in charge of a computer is authorized to issue passwords for that computer.
8. NooneshallmisrepresenthisorheridentityorrelationshiptotheInstitutewhenobtaining or using Institute's computer or network privileges.
9. No one without specific authorization shall read, alter, or delete any other person's computer files or electronic mail. This rule applies regardless of whether the operating system of the computer permits these acts.
10. No one shall copy, install, or use any software or data files in violation of applicable copyrights or license agreements, including but not limited to downloading and/or

distribution of music, movies, or any other electronic media. No one shall create, install, or knowingly distribute a computer virus, "Trojan horse," or other surreptitiously destructive program on any University computer or network facility, regardless of whether any demonstrable harm results.

11. No one without proper authorization shall modify or reconfigure any Institute's computer or network facility.
12. No one shall store confidential information in computers or transmit confidential information over Institute networks without protecting the information appropriately.
13. Users shall take full responsibility for data that they store in Institute's computers and transmitthroughnetworkfacilities.NooneshalluseInstitute'scomputersornetworkfacilities to store or transmit data in ways that are prohibited by law or Institute's policy. Users shall not transmit any communications that are harassing or discriminatory.
14. Those who publish web pages or similar information resources on Institute's computers shall take full responsibility for what they publish; shall respect the acceptable use conditions for the computer on which the material resides; shall obey all applicable laws; and shall not publish commercial advertisements without prior authorization. References and links to commercial sites are permitted, but advertisements, and especially paid advertisements are not. Users shall not accept payments, discounts, free merchandise or services, or any other remuneration in return for placing anything on their web pages or similar information resources.
15. Users of Institute's computers shall comply with the regulations and policies of mailing lists, social media sites, and other public forums through which they disseminate messages.
16. IT team and Lab Managers shall perform their duties fairly, in cooperation with the user community, the appropriate Institute administration, Institute's policies, and funding sources. It Team and Lab Managers shall respect the privacy of users as far as possible and shall refer all disciplinary matters and legal matters to appropriate authorities.
17. Email and other electronic messaging technologies are intended for communication between individuals and clearly identified groups of interested individuals. No one without prior authorization shall use Institute's facilities to knowingly create or disseminate spam -- unwanted and unsolicited emails or materials, in such a large volume that it may disrupt the proper functioning of the Institute's information technology resources or individuals' ability to use such resources. The University reserves the right to discard incoming mass mailings and spam without notifying the sender or intended recipient.
18. For its own protection, the Institute reserves the right to block communications from sites or systems that are involved in extensive spamming or other disruptive practices, even though this may leave Institute's computer users unable to communicate with those sites or systems.

5. Policy Compliance

Each department/unit of the Institute is responsible for implementing, reviewing and

monitoring internal policies, practices, etc. to assure compliance with the Institute's Policies on the Use of Computers.

The IT team is responsible for enforcing this policy, and is authorized to create technical and security standards for Institute's computing and network facilities and protection standards for information stored or transmitted by computing and network facilities of the Institute. Non Compliance

An employee/student found to have violated this policy may be subject to disciplinary action.

Systems and accounts that are found to be in violation of this policy may be removed from the Institutes network, disabled, etc. as appropriate until the systems or accounts can comply with this policy.

6. Definitions

University computers and network facilities - all computers owned or administered by any part of The B S A Crescent Institute of Science and Technology or connected to the Institute's communication facilities, including departmental computers, and also all of the Institute's computer network facilities accessed by anyone from anywhere.

Authorization- permission granted by the appropriate part of the Institute governance and/or management structure, depending on the particular computers and/or network facilities involved and the way they are administered.

2. Router and Switch Security Policy

1. Overview

See Purpose.

2. Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a Institute's network on behalf of B S A Crescent Institute of Science and Technology.

3. Scope

All employees, contractors, consultants, temporary and other workers at B S A Crescent Institute of Science and Technology must adhere to this policy. All routers and switches connected to B S A Crescent Institute of Science and Technology networks are affected.

4. Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches can use Industry standard authentication protocols for all user authentications.
2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
3. The following services or features must be disabled:
    - Incoming packets at the router/switch sourced with invalid addresses
    - All web services running on router
4. The following services should be disabled unless a proper justification is provided: B S A Crescent Institute of Science and Technology discovery protocol and other discovery protocols
    - Dynamic trunking
    - Scripting environments, such as the TCL shell
5. The following services must be configured:
    - Password-encryption
    - NTP configured (Clock Synchronization)
6. All routing updates shall be done using secure routing updates.
7. Use standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
8. The router should be included in the monitoring system with a designated point of contact
9. Each router must have the following statement presented for all forms of login whether remote or local:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You

must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring." – Content with modification to be pushed into all ICT network devices

10. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path.
11. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
12. The router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
    - Device logging
    - Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped

5. Policy Compliance

1. Compliance Measurement

   The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

   Any exception to the policy must be approved by the IT team in advance.

3. Non-Compliance

   An employee/student found to have violated this policy may be subject to disciplinary action.

6. Definitions and Terms

None.

3. Removable Media Policy

1. Overview

Removable media is a well-known source of infections and has been directly tied to the loss of sensitive information in many organizations.

2. Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by B S A Crescent Institute of Science and Technology and to reduce the risk of acquiring infections on computers operated by B S A Crescent Institute of Science and Technology.

3. Scope

This policy covers all ICT Hardware equipment (operating in B S A Crescent Institute of Science and Technology.

4. Policy

B S A Crescent Institute of Science and Technology staff may only use Institute's removable media in their work computers. Institute's removable media may not be connected to or used in computers that are not owned or leased by the Institute without explicit permission of the Director/IT Team. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state agencies. When sensitive information is stored on removable media, it must be encrypted.

Exceptions to this policy may be requested on a case-by-case basis by the IT Team to the respective Department authority.

5. Policy Compliance

1. Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to the policy must be approved by the IT team in advance.

3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

6. Definitions andTerms

- Encryption - Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.
- Malware - A generic term for a number of different types of malicious code.
- Removable Media - Removable media is a portable storage medium that allows users to copy data to it and then take it off site, and vice versa.
- Sensitive Information - Sensitive information is any unclassified information that, if compromised, could adversely affect the institute initiatives.

4. Data Protection Policy

1. Overview

Data Security is a necessary part of security policies of the Institution as incorrect use, storage and transmission of institutional or personal data held by the institute, could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

2. Purpose

This document sets out the Institute's policy on the storage, transmission and use of personal data and sensitive business information outside the institute, including on mobile devices and portable storage media.

Its aim is to ensure that the University complies with that sensitive information is protected from unauthorized access, dissemination, alteration or deletion.

3. Scope

This policy applies to all employee and student community who store, transmit and use personal data and sensitive institutional data, either in electronic format or paper format, outside the campus, including using mobile devices, portable storage media or other forms of communication. All users with access to institutional data are required to protect these data appropriately. Likewise, the Data owner must grant formal approval for the access and use of institutional data.

4. Policy

In order to maintain the security of institutional data, all data stored, processed, or transmitted must be protected in accordance with this requirement. Based on classification; users are required to implement appropriate security controls.

All Institutional data must be classified into one of the two following categories.

Public Data: Data that may be disclosed to the general public without harm.

- protect individuals' Personal Data
- be clear about how Personal Data must be Processed and the University's expectations for all those who Process Personal Data on its behalf
- Process Personal Data effectively and efficiently to achieve the purposes for which it was obtained
- protect the University's reputation by ensuring the Personal Data entrusted to it is Processed in accordance with Data Subjects' rights
- protect the University from risks of Personal Data Breaches and other breaches of Data Protection Law and hence from liability

Private Data: Data that should be kept confidential. Access to these data shall require authorization and legitimate need-to-know. Privacy may be required by law or contract.

- Access shall be limited to authorized officials or agents with a legitimate academic or business interest and a need to know as outlined by Institution policies.

- All access shall be approved by an appropriate data owner and tracked in a manner sufficient to be auditable. Before granting access to external third parties, contractual agreements which outline responsibilities for security of the data shall be approved through the institution contract process.
- Private Data is typically not subject to open records disclosure. However, some open records requests can be fulfilled by redacting sensitive portions of records. Individuals who receive a request must coordinate with Data owner/IT team.

  Data Breach: In the event of a data breach, it must be notified immediately to the IT Team of the Institution. The IT Team will be responsible for conducting or coordinating the investigation, making, or assessing recommendations for corrective action, reporting the incident administrative units as needed and maintaining documentation of the incident.

5. Policy Compliance

1. Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to the policy must be approved by the IT team in advance.

3. Non-Compliance

Confirmed violations of this policy will result in consequences commensurate with the offense, up to and including student status, or other relationships with the institution.

5. Lab Security Policy

1. Overview

See Purpose.

2. Purpose

This policy establishes the information security requirements to help manage and safeguard lab resources and Institutes networks by minimizing the exposure of critical infrastructure and information assets to threats that may result from unprotected hosts and unauthorized access.

3. Scope

This policy applies to all employees, contractors, consultants, temporary and other workers at B S A Crescent Institute of Science and Technology and its subsidiaries must adhere to this policy. This policy applies to all labs owned and managed by B S A Crescent Institute of Science and Technology.

4. Policy

- Lab owning departments are responsible for assigning lab admins, appoint of contact (POC),and a Secondary POC for each lab. Lab owners must maintain up-to-date POC information with IT. Lab admins or the secondary POC must be available around-the-clock for emergencies.
- Lab admins are responsible for the security of their labs and the lab's impact on the Institute's networks.
- Lab managers are responsible for the lab's compliance with all security policies of the Institute.
- No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by the Dean/Head of the Institute.
- Any lab that wants to add an external connection must provide a proper documentation to IT team with justification, the equipment, and the IP address space information. IT Team will review for security concerns and must approve before such connections are implemented.
- Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the network. These activities must be restricted within the lab.
- IT team reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.
- Lab Manager/Head of the Department is responsible for Physical security of the devices (PCs, Laptops, Printers, Network Devices, other lab equipment) in their labs and the department.

5. Policy Compliance

1. Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to the policy must be approved by the IT Team in advance.

3. Non-Compliance

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

6. Definitions and Terms

- Firewall - A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.

6. Anti-Virus Policy

1. Overview

See Purpose.

2. Purpose

To establish requirements which must be met by all computers connected to B S A Crescent Institute of Science and Technology networks to ensure effective virus detection and prevention.

3. Scope

This policy applies to all B S A Crescent Institute of Science and Technology computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers, and any PC based lab equipment such as traffic generators.

4. Policy

All computers of B S A Crescent Institute of Science and Technology must have Institute's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti- virus software and the virus pattern files must be kept up-to-date. Any activities with the intention to create and / or distribute malicious programs into Institute's networks are prohibited

5. PolicyCompliance

a. Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

b. Exceptions
Any exception to the policy must be approved by the IT team in advance.

c. Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions andTerms

None

7. Wireless Communication Policy

1. Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

2. Purpose

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to institute network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the IT team are approved for connectivity to the institution network.

3. Scope

All employees, contractors, consultants, temporary and other workers at B S A Crescent Institute of Science and Technology, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of B S A Crescent Institute of Science and Technology must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to the institution network or reside on the campus site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

4. Policy

All wireless infrastructure devices that reside at the institute site and connect to the institute network, or provide access to information classified as Confidential, or above must:

- Abide by the standards specified in the *Wireless Communication Standard*.
- Be installed, supported, and maintained by an approved support team.
- Use institute approved authentication protocols and infrastructure.
- Use institute approved encryption protocols.
- Not interfere with wireless access deployments maintained by institute.

5. Policy Compliance

a. Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

b. Exceptions
Any exception to the policy must be approved by the IT team in advance.

c. Non-Compliance: Confirmed violations of this policy will result in consequences commensurate with the offense, up to and including termination of employment, student status, or other relationships with the institution.

6. Definitions and Terms

MAC Address - A physical address; a numeric value that uniquely identifies that network device from every other device on the planet.

8. Remote AccessPolicy

1. Overview

Remote access to our institute network is essential to maintain, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than the institute's network. While these remote networks are beyond the control of Hypergolic Reactions, we must mitigate these external risks the best of our ability.

2. Purpose

The purpose of this policy is to define rules and requirements for connecting to institute's network from any host. These rules and requirements are designed to minimize the potential exposure to the institutional assets from damages which may result from unauthorized use of institution resources. Damages include the loss of sensitive or confidential data, intellectual property, damage of public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.

3. Scope

This policy applies to all employees, contractors, vendors and agents with a institute owned or personally-owned computer or workstation used to connect to the institute network. This policy applies to remote access connections used to do work on behalf of the institution, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to the institution network

4. Policy

It is the responsibility of employees, contractors, vendors and agents of the institution, with remote access privileges to institution's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the institute.

Requirements

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases.
- Authorized Users shall protect their login and password, even from family members.
- While using a institute-owned computer to remotely connect to institute's network,

Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

- Use of external resources to conduct institute business must be approved in advance by IT team and the appropriate department.
- Personal equipment used to connect to institute's networks must meet the requirements of institute-owned equipment for remote access.

5. Policy Compliance

a. Compliance Measurement

The IT Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

b. Exceptions

Any exception to the policy must be approved by Remote Access Services and the Infosec Team in advance.

c. Non-Compliance

Confirmed violations of this policy will result in consequences commensurate with the offense, up to and including student status, or other relationships with the institution

B.S. Abdur Rahman Crescent Institute of Science & Technology
Deemed to be University u/s 3 of the UGC Act, 1956
GST Road, Vandalur, Chennai 600 048

9. Email Policy

1. Overview

Electronic email is pervasively used in almost all verticals and is of tenth e primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it' s important for users to understand the appropriate use of electronic communications.

2. Purpose

Thepurposeofthisemailpolicyistoensuretheproperuseofinstitutionemailsystemandmakeu sers aware of what the institution deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within Institute Network.

3. Scope

This policy covers appropriate use of any email sent from the institute's email address and applies to all employees, vendors, and agents operating on behalf of B S A Crescent Institute of Science and Technology.

4. Policy

- All use of email must be consistent with the policies of the institution and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- Institute email account should be used primarily for institute related purposes; personal communication is permitted on a limited basis, but commercial uses are prohibited.
- All data pertaining to the institute, contained within an email message or an attachment must be secured according to the *Data Protection Policy*.
- Email should be retained only if it qualifies as a institute's business record. Email is a institute business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

- The institute email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Members of the community who receive any emails with this content from any other employee/ student should report the matter to their department Head / Director – Data centre immediately.

Users are prohibited from automatically forwarding institute email to a third party email system. Individual messages which are forwarded by the user must not contain confidential information of the institute.

- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct institute business, to create or memorialize any binding transactions, or to store or retain email on behalf of the institution. Such communications and transactions should be conducted through proper channels using institute-approved documentation.
- Using a reasonable amount of institute resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from the institute email account is prohibited.
- Institute employees/students shall have no expectation of privacy in anything they store, send, or receive on the company's email system.
- Institute may monitor messages without prior notice. Institute is not obliged to monitor email messages.

5. Policy Compliance

a. Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

b. Exceptions

Any exception to the policy must be approved by the IT team in advance.

c. Non-Compliance

Confirmed violations of this policy will result in consequences commensurate with the offense, up to and including termination of employment, student status, or other relationships with the institution

Abbreviations

Abbreviation	Full Form	Remarks
TCL	Tool Command Language	Scripting Language which could be used for network programming
NTP	Network Time Protocol	Networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
SNMP	Simple Network Management Protocol	**SNMP** is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
RFC1918 addresses	Request For Comments	Private Network Addresses
POC	Point of Contact	
IT	Information Technology	
ICT	Information Communication Technology	
MAC	Medium Access Control	
VPN	Virtual Private Network	

Contact Information

For all requests, reach out to Data centre Team and for all approvals and escalations please reach out Director – Data centre.

Revision History

Date of Change	Version Number	Section	Done By	Summary of Change
22-12-2020	v1.0	All	IT &Software Policy Committee and Data Centre Team	Creation of IT Security Policy

B.S. Abdur Rahman Crescent Institute of Science & Technology
Deemed to be University u/s 3 of the UGC Act, 1956
GST Road, Vandalur, Chennai 600 048

Website Policy

Overview

A website reflects an institution's identity and is often the first point of contact for prospective students, faculty, researchers and others. The website is a tool for selling the institution and its values, so the design, content and features should be viewed accordingly. Having the right content, language, user experience, accessibility and effectiveness for an international audience is especially important now, as internationalization is an integral part of higher education's continuous change process. The website of the institution offers powerful opportunities for expanding it’s global reach and reputation. In order to have this in place a Policy for Institute website is mandatory.

Purpose

The purpose of this document is to create a Policy for the design, contents and maintenance of the website. The necessary actions required for the availability and security of the website should also be mentioned in the policy.

Scope

The policy for design and maintenance of the website applies primarily to a larger extent to the website maintenance team and the Data Centre. This policy covers the design, contents, maintenance and security of the website as a whole which includes the information of every section of the Institution.

Design and Content Policy

The purpose of the BSACIST website design and contents policy is to ensure that the website maintenance team and the Data Centre are aware of the design and contents procedure and the way they maintain it. The objective of this policy is to define the roles, responsibilities and critical elements for the efficient operations and support of Institution website.

All the contents of the website should be provided by the concerned head of the division / department / school through proper approval.

Maintenance Policy

The maintenance policy of the Institute website should address the following:

- Thoroughly review and test the entire website (annually or after any updates).
- Test the website forms/checkout process (quarterly or after any updates).
- Security updates and bug fixes (monthly or as patches are released).
- Renew the domain names (annually).
- Check backups (annually).
- Test browser compatibility (annually).
- Update dates and copyright notices (annually).
- Review contact information (annually or as needed).
- Review and update legal disclaimers (annually).

The division / department / school wants to update the contents of their page, they can send the updated contents through official email to the website maintenance team. This updates to be done will be assigned to a staff member by the head of website maintenance team / Director, Data centre.

The assigned Staff member will respond to updation of webpage content requests submitted to the website maintenance team. If a request cannot be processed within the stipulated timeframe, the Staff should inform the sender who submitted the request and the Director, Data Centre about the issue.

Once the website maintenance team receives the mail it will use the following guidelines to prioritize its response to requests:

Priority	Criteria	Response Time (During working hours only)
Critically High	Requests for issues having a significant and immediate impact on the Institution's operations. For example: • An issue affecting all or a large number of users. • An issue preventing users to access critical applications or data or impacting critical functions (e.g. emergency holiday, important events, etc). • An information security incident or vulnerability with a critical/high severity/risk.	**30 minutes**
High	Requests for issues having an important impact on the Institution's operations. For example: • Webpage error affecting a division / department / school. • An issue impacting important functions of a division. • An information security incident or vulnerabilities with a medium/high severity/risk. • Others as directed.	**2 hours**
Normal	Requests for issues having a limited or non-immediate impact on the Institution's operations. For example: • An update request for contents of a division / department / school. • An issue impacting a non-critical function in a system • A security incident or vulnerability with a low/medium severity/risk.	**Before the end of the next working day**
Low	Issues that have no material or immediate impact on the Institution's operations. For example: • A request, to improve the look and feel of a page of particular division / department / school or a minor non-functional change to the page. • Update request for faculty profile content or any other content which is not urgent.	**Two to Five working days.**

Procedure Compliance

- The staff members should send the information to be displayed / updated on the website only through proper approval from concerned heads of divisions / departments / schools.
- The updation of website contents should be done by the website maintenance team, only after receiving request from an authorized person.
- Strict action will be taken against the staff member if any content updation is done that comes from an unauthorized person.

Performance Indicators and Metrics

The following performance indicators and metrics will be used by the Director Data centre and the team to monitor the website and incidents:

- Number of total problems and incidents by severity (and category where applicable)
- Number of problems and incidents resolved
- Number of problems and incidents unresolved, with the time since opened and description of why they are still open
- Average time to resolve problems and incidents

Contact Information

For all requests, reach out to Website Maintenance Team and Data centre Team through proper channel.

Revision History

Date of Change	Version Number	Section	Done By	Summary of Change
22-12-2020	v1.0	All	IT &Software Policy Committee and Data Centre Team	Creation of Website Policy

B.S. Abdur Rahman Crescent Institute of Science & Technology
Deemed to be University u/s 3 of the UGC Act, 1956
GST Road, Vandalur, Chennai 600 048

IT Maintenance policy

Overview

In modern world the usage of Information and Communications Technology (ICT) Software is unavoidable and for institutions like BS Abdur Rahman Crescent Institute of Science & Technology (BSACIST) the need is more to keep up with technology in order to have the students trained. In order to have this in place a Policy for Software Usage, purchase, installation, maintenance and Management is mandatory

Purpose

The purpose of this document is to create a Policy for the maintenance of Software, Hardware Network and the maintenance of the security of the software services (like email, FOSS etc.).

Scope

This maintenance policy applies primarily to a larger extent to the staff of the computer maintenance cell and the Data Centre and to some extent all members of the institution including students, teaching staff, non-teaching staff, visiting faculties, vendors and contractors. This policy covers the maintenance all Institution offices, including specifically the data centre and all IT systems or applications managed by the Institution that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

Maintenance Policy

The purpose of the BSACISTICT maintenance Policy is to ensure that BSACIST employees are specially the computer maintenance cell and the data centre are aware of the maintenance procedure and the way the handle it. The objective of this policy is to define the roles, responsibilities and critical elements for the efficient operations and support of IT systems at the Institution

Maintenance Procedure

- **IT Problems** are conditions or situations (known or unknown) that can result in an incident.
- **IT Incidents** are unplanned events which cause an interruption to, or a reduction in, the quality of the IT operations or services.
- **Security Vulnerabilities** are IT problems that present specific risks to cyber security.
- All stakeholders must protect IT assets against the threats of: unauthorized access, theft, loss, or destruction
- Vulnerabilities that have a high probability of being exploited and that will highly impact the Institution (risk of operation disruption, data breach, etc.) are often labeled as **Critical** or **High**.
- The IT service Desk will act as the central point of contact for all IT technical requests.
  - ✓ The person facing any technical glitch can send a mail regarding the issue to the IT services desk. This issue will be assigned to a IT staff by the Director, Data centre
  - ✓ The assigned IT Staff will respond to the requests submitted to the IT Help Desk. If a request cannot be processed within the stipulated timeframe, the IT Staff should inform the user who submitted the request and the Director, data centre about the issue.
  - ✓ If the incident is not able to be resolved by the Data centre team, it will be escalated to the OEM / Vendor for additional assistance for closure.
  - ✓ Once the IT service Desk receives the mail it will use the following guidelines to prioritize its response to requests:

Priority	Criteria	Response Time
Critically High	Requests for issues having a significant and immediate impact on the Institution's operations. For example: □ An issue affecting all or a large number of users. □ An issue preventing users to access critical applications or data, or impacting critical functions (e.g. access to network shares, email, or academic courses). □ An information security incident or vulnerability with a critical/high severity/risk. □ An issue affecting the ability of a class to be delivered or a meeting to take place. □ Other as directed (removal of access rights for an unscheduled terminated user for example).	< 1 Hr
High	Requests for issues having an important impact on the Institution's operations. For example: □ An application error affecting a small group of users. □ An issue impacting important functions in a system. □ An information security incident or vulnerabilities with a medium/high severity/risk. □ Other as directed	**4 hours**
Normal	Requests for issues having a limited or non-immediate impact on the Institution's operations. For example: □ An issue affecting one person only. □ An issue impacting a non-critical function in a system (reporting for example). □ A security incident or vulnerability with a low/medium severity/risk. □ A question on how to use a non-critical functionality.	**Before the end of the next working day**
Low	Issues that have no material or immediate impact on the Institution's operations. For example: □ A "cosmetic" request, to improve a system functionality "look and feel" or a minor non-functional change to a system	**More than two working days. Within a week if possible.**

Procedure Compliance

- Where possible, the ICT team will take preventative measures to prevent problems from occurring and minimize the impact of incidents that do occur by addressing identified problems as quickly as possible. Examples of preventative measures include the implementation of high availability and redundant systems and back-up solutions.
- Mandatorily wherever required, the ICT assets will be covered under AMC (Annual Maintenance Contract) for providing an higher availability to the campus network
- ICT Assets purchased newly to be covered via additional warranty for proper maintenance of the equipment's or software.
- Problems and incidents with a priority of urgent or high must be reported within four hours of detection to contain the issue, and if possible, prevent any further impact.
- The Director Data centre and their team can conduct investigations into problems and incidents with priorities of urgent or high to determine the root cause of the issues, to take proactive measures.
- The following performance indicators and metrics will be used by the Director Data centre and the team to monitor IT problems and incidents:
    - ❖ Number of total problems and incidents by severity (and category where applicable)
    - ❖ Number of problems and incidents resolved
    - ❖ Number of problems and incidents unresolved, with the time since opened and description of why they are still open
    - ❖ Average time to resolve problems and incidents

Keywords and Abbreviations

KEYWORD	DEFINITION
IT	Information Technology
ICT	Information and Communications Technology
Software	General term used for Software including Operating Systems, Office usage Software, LAB Software, Open Source Software etc.

Hardware	General term used for hardware including Routers, Switches, Firewalls, Servers, Storage, Desktops, Laptop, Printers and Scanners
AMC	Annual Maintenance Contract

Contact Information

For all requests, reach out to Data centre Team and for all approvals and escalations please reach out Director – Data centre.

Revision History

Date of Change	Version Number	Section	Done By	Summary of Change
22-12-2020	v1.0	All	IT &Software Policy Committee and Data Centre Team	Creation of IT Maintenance Policy