CENTRE FOR NANO SCIENCE AND ENGINEERING

# *INFORMATION TECHNOLOGY PROCESS*

*(Released: Date_30 Jan 2024; Version 1.0)*

## Contents

## Objective

The objective of the IT Handbook is to manage and support the Information Technology's infrastructure and services of the Centre for Nano Science and Engineering (Hereinafter known as "CeNSE").

## Purpose

This handbook will be focused on providing guidance on information technology (IT) operations that directly impact the daily business operations. This document aims to provide the standards and best practices to be followed.

## Governance, Compliance and Authority

The CeNSE Management fully supports this Process. CeNSE Information Security is responsible for managing and administering this standard for all CeNSE.

This document is subject to periodic review and revision. The current online version supersedes all previous versions.

## Scope

This applies to all at CeNSE.
Location unit I: MNCF (Micro and Nano Characterization Facility)
Location unit II: NNFC (National Nanofabrication Centre)

## Information Security (IS)

The purpose of IS policy, standards, processes, and procedures are to establish and maintain a standard of due care to prevent misuse or loss of CeNSE information assets. Standards are the specifications that contain measurable, mandatory rules to be applied to a process, technology, and/or action in support of a policy.

CeNSE must provide for the integrity and security of its information assets by creating appropriate internal policies, processes, standards, and procedures for preserving the integrity and security of each automated paper file or database.

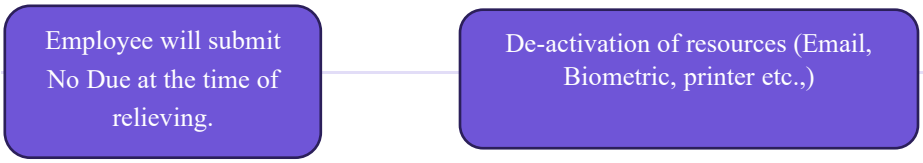
**Each CeNSE employee must**:

1. Establish and maintain management and staff accountability for the protection of CeNSE information assets.
2. Establish and maintain processes for the assessment and analysis of risks associated with CeNSE information assets.
3. Establish appropriate administrative policies, processes, and procedures to protect and secure IT infrastructure,

## Allocation of IT Resources

### Employee Onboarding


### Employee Offboarding




### Appropriate IT Use Policy

Preserving access to information resources is a system-wide effort that requires each user to act responsibly and guard against abuses. Therefore, the CeNSE and its users have an obligation to abide by the following standards of appropriate and ethical use:

-Use only those IT resources for which you have authorization
-Protect the access and integrity of IT resources
-Abide by applicable local, federal laws and Indian Institute of Science (IISc) policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted material.
-Use IT resources only for their intended purpose
-Respect the privacy and personal rights of others
-Zero tolerance to piracy
-Do no harm

Failure to comply with the appropriate use of these resources threatens the atmosphere for the sharing of information, the free exchange of ideas, and the secure environment for creating and maintaining information property, and subjects one to disciplinary actions. Any user of CeNSE, including that of NNFC and MNCF found using IT resources for unethical and/or inappropriate practices has violated this policy and is subject to disciplinary proceedings, including suspension of system privileges, termination of employment and/or legal action as may be appropriate. Although all members of the CeNSE have an expectation of privacy, if a user is suspected of violating this policy, his or her right to privacy may be superseded by the CeNSE 's requirement to protect the integrity of IT resources, the rights of all users, and the property of the CeNSE.

## Computing Devices Hardware and Software

*Guidelines*

1. All computing devices will run Windows Defender/antivirus software and its auto updating agent, if available.
2. Every end user computing device will run an official operating system that is updated at the regular defined cycle, unless there is reason not to upgrade to the latest patches. This will be Windows 7/10 for all operations and Windows 10 for newly deployed workstations and laptops. There might be some systems running open-source Linux or other required operating systems as per project needs.
3. It is unacceptable to run unlicensed copies of software on any CeNSE machines. Non-compliance will lead to disciplinary action.
4. Because not everyone is technically knowledgeable to ensure that computers are properly maintained, automatic processes and/or designated personnel may be dispatched to perform these updates.
5. Computer workstations and network resources shall be used only for work-related activities. Non-work-related usage of the computing device is prohibited.

## Infected/Compromised Machines

All machines that are compromised must have their disks reformatted and the operating system and other programs reinstalled from scratch. When the machine is rebuilt, it must not be deployed until all software patches have been applied. Rebuilding computers from scratch is the only way to guarantee that all hacker-written software is removed.

## Security

CeNSE employs various measures to protect the security of its computing resources and its user's accounts. Users should be aware, however, that the CeNSE cannot guarantee the absolute security and privacy of data stored on CeNSE computing facilities. Users should, therefore, engage in safe computing practices including establishing appropriate access restrictions to their accounts and not leaving their account logged on after they leave their station.

Users should not share any login information nor write it down on any support. The password confidentiality will be preserved. Users will change their password regularly and make sure the passwords used are strong. They will also encrypt and back up critical files when appropriate.

When disposing of computers, servers, or other hardware, cense will totally wipe out all data on these devices. In as much as possible, a complete reformat is to be executed. If there are no major financial drawbacks, the data carriers should be physically destroyed.

## User Responsibilities

Use of CeNSE IT resources is granted based on acceptance of the following specific responsibilities:

Use only those computing and IT resources for which you have authorization. For example, it is a violation:

-To use resources, you have not been specifically authorized to use

-To use someone else's account and password or share your account and password with someone else

-To access files, data, or processes without authorization

-To purposely look for or exploit security flaws to gain system or data access

Protect the access and integrity of computing and IT resources. For example, it is a violation:

-To use excessive bandwidth

-To release a virus or a worm that damages or harms a system or network

-To prevent others from accessing an authorized service

-To send email that may cause problems and disrupt service for other users

-To attempt to deliberately degrade performance or deny service

-To corrupt or misuse information

-To alter or destroy information without authorization

Abide by applicable laws and CeNSE policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software. For example, it is a violation:

-To download, use or distribute copyrighted materials, including pirated software or music or videos or games

-To make more copies of licensed software than the license allows

-To upload, download, distribute, or possess pornography

Use computing and IT resources only for the intended purposes. For example, it is a violation:

-To use computing or network resources for advertising or other commercial purposes

-To distribute copyrighted materials without express permission of the copyright holder

-To send forged email

-To misuse communications software to allow users to hide their identity, or to interfere with other systems or users

-To send terrorist threats or “hoax messages”

-To send chain letters

-To intercept or monitor any network communications not intended for you

-To attempt to circumvent security mechanisms

-To use former privileges after transfer or termination, except as stipulated by the CENSE Policies and Procedures

Respect the privacy and personal rights of others. For example, it is a violation:

-To use electronic resources for harassment or stalking other individuals

-To tap a phone line or run a network sniffer or vulnerability scanner without authorization

-To access or copy another user’s electronic mail, data, programs, or other files without permission

-To disclose information about employees in violation of CeNSE Guidelines

## System and Network Administrator Responsibilities

System Administrators and providers of CeNSE computing and IT resources have the additional responsibility of ensuring the confidentiality, integrity, and availability of the resources they are managing. Persons in these positions are granted significant trust to use their privileges appropriately for their intended purpose and only when required to maintain the system.

## Security Caveat

Be aware that although computing and IT providers throughout the CeNSE are tasked with preserving the integrity and security of resources, security sometimes can be breached through actions beyond their control. Users are therefore urged to take appropriate precautions such as:

- Safeguarding their account and password
- End users must take their own backup of desktop/laptop data as per project need.
- Taking full advantage of file security mechanisms
- Backing up critical data regularly; now this is defined as data from File server; data. a backup policy to be informed to all stakeholder with backup available within certain time frame only. Every project owner must make sure that they take data backup of their critical data at their end.
- Promptly reporting any misuse or violations of the policy

### Email Account use policy.

To increase the efficient distribution of critical information to all faculty, staff and students, and the Institute's administrators, it is recommended to utilize the university's e-mail services, for formal Institute communication and for academic & other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal Institute communications are official notices from the Institute to faculty, staff, and students. These communications may include administrative content, such as human resources information, policy messages, general Institute messages, official announcements, etc.

CeNSE IT coordinates with the Institute's central email support team to provide a new email account to the user. Users may know that by using the email facility, they agree to abide by the policy followed by the Institute's central email support team. Click here for more information

## Biometrics

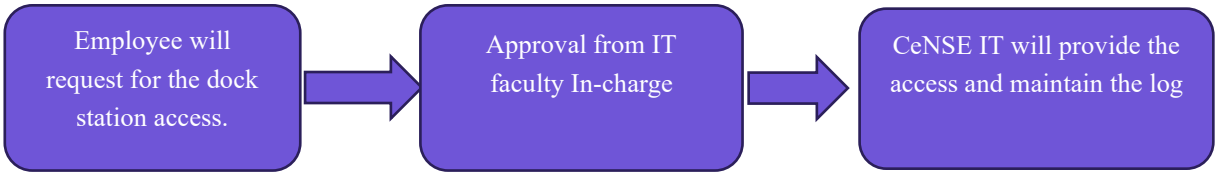
The Centre for Nano Science and Engineering is using a Facial biometrics system for main door and all other rooms. IT along with CeNSE infrastructure team handles this operation.

User will register to Biometric through online portal, on approval from concerned Manager/faculty, Biometric is assigned.

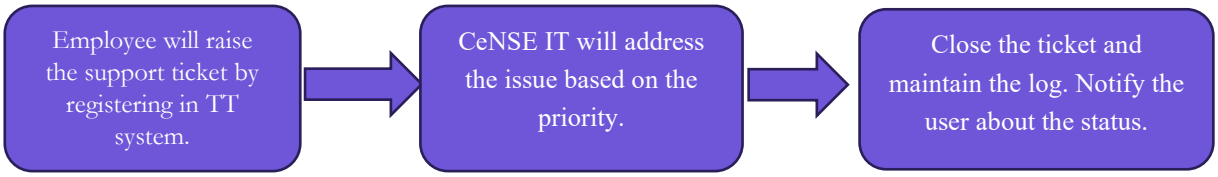
**Basic Monitoring Tasks**

- Attendance management
- Download time stamps upon request for investigations.
- De-active the account once employee is relieved.
- Monitor active and inactive biometrics registrations.

## Dock Station Access



## CeNSE TT System (CeNSE trouble ticketing system)




## Server Level support

- Storage Server – where users / projects store their data via FTP access. Access rights are given to specific users only.
- WINSCP: FTP / Intel server – maintained and monitored by IT, with FTP Access given to authorized users to access their data if required.
- FOM and website servers: These servers are managed by IT and respective backup is taken.

## Maintenance check and audit of assets

A maintenance check and audit every month will be conducted by the CeNSE IT to check the following details:

- Proper functioning of the projector and displays.
- Proper functioning of Mouse, Keyboard, etc.,
- Proper functioning of central printer.
- Proper functioning of cables and wires
- Proper LAN/Wireless Network connectivity