CENTRAL ENGINEERING CONSULTANCY BUREAU

Information Technology Unit

IT Policy and Procedure Manual

Overview

This document serves as a rulebook and roadmap for properly and successfully utilizing the information technology resources at the Central Engineering Consultancy Bureau. Any misuse, misappropriation, negligence, concerning these policies and procedures will not be accepted.

It is the purpose of the CECB Information Technology Unit to provide these policies and procedures in order to address potential situations and to stipulate steps to be taken during these situations. However, not all situations can reasonably addressed without exception and therefore ever be addressed so it is up to each individual employee and affiliate to apply these policies and procedures as a principle of what type of actions are to be taken.

1. CECB IT Policies

Acceptable User Policy

Overview

This policy establishes the acceptable usage guidelines for all CECB owned information technology resources. These resources can include, but are not limited to, following equipment:

- Computers
  Desktop Computers, Servers, etc.

- Network Equipment
  Switches, Routers, Network and Communications Cabling, Wall Plates, Wireless Antennas,
  Wireless Bridge Devices, Fiber Optic Lines, Fiber Optic Equipment, etc.

- Audio/Video Equipment
  Video Codecs, HDTVs, Document Cameras, Projectors, Security Cameras, Miscellaneous Cabling, Digital Cameras, Printers, Copiers, Fax Machines, etc.

- Software
  Operating Systems, Application Software, etc.

- Resources
  Group Drive File Storage, Website File Storage, Email Accounts, etc.

This policy applies to all employees, contractors, consultants, temporary personnel, trainees and other workers at CECB, including any and all personnel affiliated with third parties, which includes vendors. This policy applies to all equipment that is owned by the CECB.

1.1 Information Technology Policy

While CECB's IT Unit desires to allow a reasonable level of freedom and privacy, users should be aware that all CECB-owned equipment, network infrastructure, and software applications are the property of CECB and therefore are to be used for official use only. Also, all data residing on CECB-owned equipment is also the property CECB and therefore, should be treated as such, and protected from unauthorized access.

The following activities provide a general roadmap for using CECB's technology resources in an acceptable manner:

1. All passwords used to access CECB systems must be kept secure and protected from unauthorized use.
2. No user account can be shared between individuals. Authorized users are responsible for the security of their own passwords and accounts.
3. No user is permitted to change user account (Domain account) settings except the System Administrator in IT unit.
4. Do not transfer personally identifiable information on portable equipment and storage devices.
5. CECB will issue a letter to all users when issuing a Laptop, Desktop, UPS etc with the conditions stipulated by the General Manager for proper well use of the issued item. Sample letter is attached for further reference.
6. All computers residing on the internal CECB network, whether owned by the employee or CECB shall continually execute approved virus scanning software with a current, up-to-date virus database.
7. Employees must use extreme caution when opening email attachments received from unknown senders.
8. Personally identifiable information shall not be sent via electronic means and should be transferred within the internal netw ork or through secure VPN connections.
9. All workstations should be kept secure.Users should lock the workstati on when unattended in order to protect unauthorized users from accessing secure files.

The following activities are, in general prohibited.

Employees may be exempted from these restrictions in the course of carrying out work of their authorized job responsibilities (eg:- systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).Under no circumstances is an employee of CECB authorized to engage in any activity that is illegal under local, state or international law while utilizing CECB -owned resources.

The following activities are strictly prohibited, without exception:

1. Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CECB.

2. Introduction of malicious programs into the network or server environments (e.g., viruses, worms, Trojan horses, root kits, etc.).

3. Revealing account passwords to others or allowing use of your account by others. This includes family and other household members if and when work is carried out at home.

4. Using a CECB computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or any workplace laws introduced by the government in the user's local jurisdiction.

5. Port scanning or security scanning is expressly prohibited unless prior sufficient notification to the CECB IT unit is made.

6. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's authorized normal job/duty.

7. Circumventing user authentication or security of any host, network or account.

8. Interfering with or denying service to any user other than the employee's host is not accepted.

9. Using any program/script/command, or sending messages of any kind with the intent of interfering with, or disabling , a user's terminal session, via any means, locally ,or via the Internet/Intranet/Extranet.

10. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who have not specifically requested such material (email spam).

11. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

12. Social media (which is a software system or service provided via the Internet used to communicate and share information between people through interactions with video, audio, text or multimedia) and also - due to lack of bandwidthTorrents sites executable files which are harmful to the LAN in CECB are not permitted.

13. In case of failures in IT related services such as Internet, Computer issues, emails etc should be directly contacted IT help desk (5353) as first level support. Help Desk coordinator shall be escalated to next level of support if required.

2. Disciplinary Action

Employees who do not adhere to the IT Policies of the CECB will face disciplinary action. Serious violations will be cause for termination of employment, or legal action when appropriate according to the CECB HR policies.

3. Auditing Policy

Overview

This policy addresses internal and third-party entities of the ability of to conduct an internal information technology audit. This type of audit is basically a "stress-test" on our information technology resources to evaluate the level of security present in our information technology systems as well as the level of scrutiny it can withstand.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate the possibility of security incidents and ensure conformance to the established CECB IT Department's security policies.
- Monitor user or system activity where appropriate.

Policy

This policy covers all computers, equipment, and communication devices owned or operated by CECB.

When requested, and for the purpose of performing an audit, consent for the access required top form the scan will be provided to members of the audit group by the CECB IT unit. The CECB IT unit will provide its consent to allow the audit group to access its networks, firewalls, and other hardware devices to the extent necessary to perform the scans authorized. The CECB IT Department shall provide protocols, addressing information and network connections sufficient for the audit group to perform network scanning.

The access involved in the scan may include:

- User level and/or system level access to any computing and networking equipment, and communications devices.
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or store in CECB equipment and/or premises
- Access to work areas (labs, offices, storage areas, etc.)
- Access to interactively monitor and log traffic on CECB networks.

4.Backup Policy

Overview

The CECB IT unit maintains systems to hold and retain all essential data for each individual department for 30 days. This storage area or group drive as it is referred to is used to securely store all data forany given department. Because of this centralized storage arrangement, the CECB IT unit is able to offer secure backup capability ensuring all data will be accessible in the event of a disaster or other event in which the data would be destroyed.

Policy

Every effort shall be made by the individual departments and employees at CECB to store sensitive, important, and confidential data on their respective group drive. As mentioned above, the CECB IT unit cannot be held liable for issues with data stored elsewhere.

Regular backup schedules are in place within the group drive storage device to ensure that backups occur at regular intervals and over a time span to provide ample opportunity for the CECB IT unit to recover a file, folder, or group of such. It should be noted that the CECB IT unit does require immediate notification in the event a file, folder, or collection of either is found to be missing, corrupt, or otherwise damaged. Delay in informing the CECB IT unit decreases the probability of successful recovery.

Backups Process

These refer to snapshots taken of the file structure and database. These snapshots are essentially pointers to changes occurring within the storage device since the last scheduled snapshot. This greatly reduces the file storage requirements necessary to hold backups while still providing the same or superior level of backup capability found in other devices. In addition to CECB IT Department performs the file level backup for each system, applications, switch configurations, firewalls etc.

Regularly scheduled back ups are performed by the CECB IT Department according to the following schedule:

- **Daily Backup**:
  Starting at 5.00 PM
- **Mid-Month Backup** :
  Starting on 15thof each month at 9.00 AM
- **Monthly Backup** :
  Starting on 1st of each month at 9.00 AM
- **Yearly Backup** :
  Starting on 31stDecemberof each year at 5.00 PM

Backup Restoration &Testing:

CECB IT performs backups are restoration and backup testing on Quarterly during for the year. It will be performing with this testing schedule.

Quarter 1: 1st – April 1-7 days
Quarter 2: 1st – July 1-7 days
Quarter 3: 1st – September 1-7 days
Quarter 4: 1st Dec – 7 th Dec.

5.Data Retention Policy

Overview

This policy will determine how long data shall be retained under the guidelines of state law and policies of the CECB and as stipulated herein.

Policy

All data shall be retained, at minimum, for the time frame as specified in any current, standing or state law. No data residing within any CECB facility or information technology equipment will knowingly be destroyed prior to this timeframe unless such laws are modified to reflect a new time frame. If such changes do occur, the new timeframe will be subject to the new law and all data will be retained within the new specifications.

This policy shall not decrease the retention time of any state law but may only increase the retention timeframe required by the CECB IT unit. This increase may only be applicable as long as it does not compromise the integrity on storage capability, or otherwise degrade the overall storage capability of the system being used.

6. Password Policy

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of CECB's entire network. As such, all CECB Employees (including contractors and vendors with access to CECB systems) are responsible for taking appropriate steps, as outlined below, to select and secure their passwords.

Policy

All passwords shall meet the following criteria:

- All system-level (excluding system accounts that are bound with applications such as cecb.lk web site, SMS application etc.) passwords must be changed at least every 90 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- User accounts that have system-level privileges granted through group memberships or programs such as ERP must have a unique password from all other accounts held by that user.
- Passwords must NOT be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines as described below.

Passwords are used for various purposes at CECB. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins.

Very few systems have proper support for one-time tokens (i.e., dynamic passwords that are only used once); therefore, every CECB employee should know how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password or a subset of the password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:

- Names of family, pets, friends, co-workers, fantasy characters, etc.

Strong passwords have the following characteristics:

- ✓ Contain between 8 and 32 characters
- ✓ Contain both upper and lower case characters (e.g., a-z, A-Z)
- ✓ Contain at least one number (e.g., 0-9)
- ✓ Contain special characters (e.g., ~, !, @, #, $, ^, (,), _, +, =, -, ?, or ,)
- ✓ Does not contain a dictionary word in any language, slang, dialect, jargon, etc.
- ✓ Does not contain personal information, names of family, etc.

All passwords are to be treated as sensitive, confidential CECB information.

Hereunder is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE.
- Don't reveal a password in an email message.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Do not use the "Remember Password" feature of applications.
- Do not write passwords down and store them anywhere in your office.

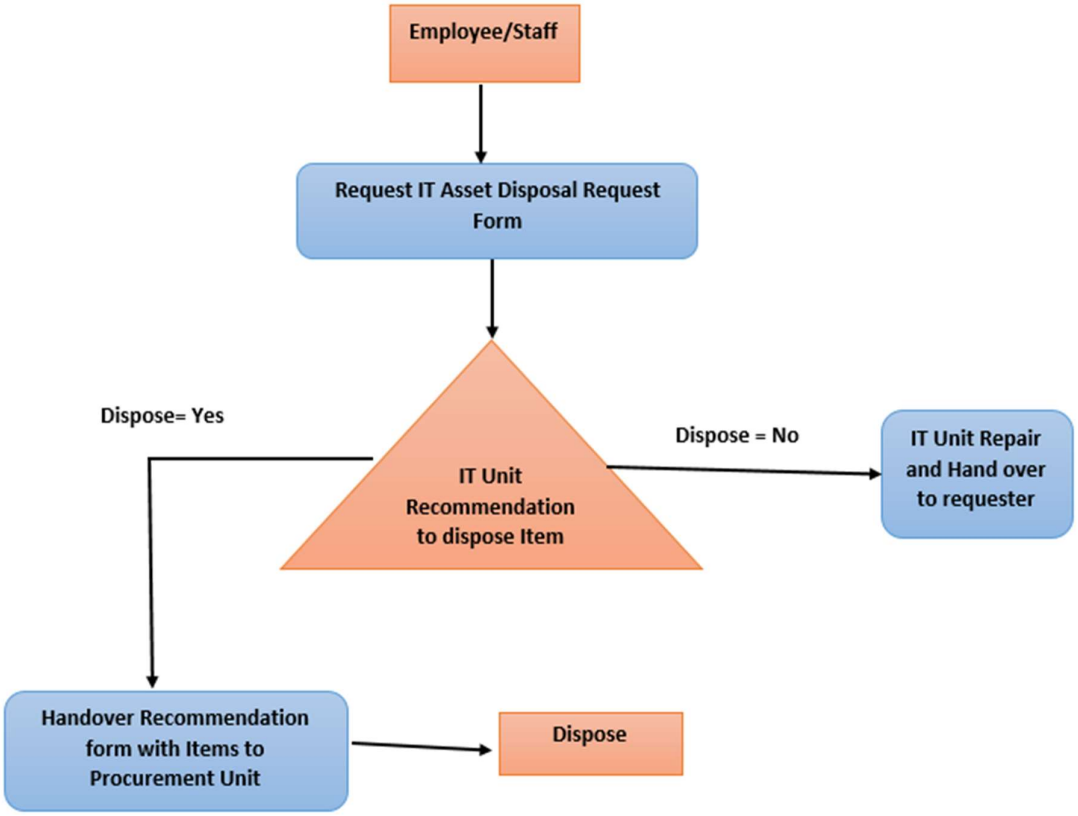
The attached form to be filled and signed and give to IT unit by Employees who are allocated Laptop Computers

7. Remote Access Policy

This policy establishes the official rules set forth to allow users to remotely access and manipulate personally identifiable information, network applications, and other data from CECB IT network.

8. IT Asset Disposal Process

All IT asset disposals must be requested via an **IT Asset Disposal Request Form** and should be completed and submitted to Procurement unit. IT asset disposal procedure is illustrated in the flow diagram.



9.Sample of IT Asset Disposal Request Form

CENTRAL ENGINEERING CONSULTANCY BUREAU

INTERNAL MEMO

To:

Date:

Through:DGM(IT)

From: **System Engineer (IT)**

Information Technology Unit Hardware Item Recommendation Report

Item Requested Employee	
Section/Unit	
Items	
Job Number	
Serial Number (#)	
Inspect Date	
Defect/Failure Item	
Item Purchase/Assembled Date	
IT Unit Recommendation	

Signature of System Engineer: …….. **Date: …….**

Signature of DGM (IT): …….. **Date: …….**

CC: Procurement Officer, Janaka Padmakumara