IT1
Category: INFORMATION TECHNOLOGY

INFORMATION TECHNOLOGY SECURITY

I. BACKGROUND

Information technology ("IT" or "Information") is a critical Monterey Bay Community Power (MBCP) asset and will be managed to ensure that it remains complete, accurate, confidential, and available only for authorized business activities. Proper management of data and information is required to support regulatory compliance, minimize legal liability, reduce the risk of criminal activity, and sustain stakeholder and customer satisfaction.

II. POLICY

Risk Exposure and Controls:
MBCP is dependent on information technology to conduct its business operations. All MBCP staff are responsible for reporting to management any non-compliance of this policy. MBCP will make information technology accessible only to authorized employees or designated vendors as needed and such information shall only be used for authorized agency purposes. To ensure protection of information technology, operational guidelines will be put in place for employees and designated vendors which adhere to the principles below:

1. Access to specific information technology is to be assigned to MBCP employees or designated vendors with the minimum level of access necessary to perform respective responsibilities.
2. Access to information technology will be made available only to the extent necessary to support authorized business functions.
3. Security systems will be structured with multiple layers of security, including physical, network, host, and personnel security measures.
4. The degree of information security protection is to be commensurate with the impact of inadvertent or intentional misuse, improper disclosure, damage or loss.
5. Adequate controls will divide sensitive duties among more than one individual to provide checks and balances that help insure operational guidelines are followed.
6. Security is not an optional component of operations. All MBCP staff and designated vendors are required to protect information. All staff and designated vendors that use or have access to MBCP information technology are personally responsible for exercising the proper control over information according to the operational guidelines provided to them.
7. Operational guidelines for treatment of information technology are subject to change as needed to protect MBCP and its customers based on any changes in systems, threats, and practices.

IT2
Category: INFORMATION TECHNOLOGY

INFORMATION SYSTEM USE POLICY

I. PURPOSE

The purpose of this policy is to outline the acceptable use of information systems and resources at MBCP. Inappropriate use exposes MBCP to risks including malware, compromise of network systems and services, and legal issues. Therefore, this policy has been put into place to protect users and MBCP.

II. SCOPE

All users of MBCP's computers or network infrastructure.

III. DEFINITIONS

"Data" is any and all information stored or transmitted over MBCP Resources.

"Information Systems" refers to all Resources that store, transmit or present information related to MBCP business.

"Resources" refers to all MBCP-owned hardware and software including, but not limited to:

- Computers, laptops, tablets, desk phones
- Monitors, printers, scanners,
- Network storage, network infrastructure, servers
- All software applications licensed by MBCP
- Accounts such as email account or other accounts used to access MBCP applications
- Data plans, subscription services
- Audio and video equipment

"Sensitive Information" includes all Data, in its original and duplicate form, which contains personal information, protected health information, customer record information, card

holder Data, confidential personal Data, or information that is deemed to be confidential or is otherwise exempt from disclosure under state law.

“User” is anyone using MBCP computing Resources including, but not limited to: employees, contractors, limited-term employees, and interns.

IV. POLICY

A. ACCEPTABLE USE

Use of MBCP’s Information Systems is limited to MBCP business.

You may access, use or share MBCP proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

B. STRICTLY PROHIBITED USE

Use of MBCP Information Systems to send messages of a threatening, harassing, or obscene nature, or any behavior found to be inconsistent with the MBCP Employee Handbook, is prohibited. Inappropriate use may include, but is not limited to: the display or transmission of sexually explicit images, messages or cartoons, any transmission that contains ethnic slurs, racial epithets, or anything that constitutes harassment or disparagement of others based on their race, national origin, color, sex, sexual orientation, age, disability, religious or political beliefs.

Violations 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 MBCP.

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources,

copyrighted music, and the installation of any copyrighted software for which MBCP or the end user does not have an active license is strictly prohibited.

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

C. SECURITY AND PERSONAL INFORMATION

All software applications and subscription services are to be secured with a password sufficient to protect MBCP information. Users who are granted access to any part of MBCP's Information Systems are provisioned with an account.

Users are to use their assigned account and no other.

Users are prohibited from using another User's account to access any part of an Information System.

Users are prohibited from sharing their passwords or passphrases. Authorized staff may reset passwords as required for business purposes. Users who are provisioned with MBCP Resources are not allowed to change permissions, modify hardware, or modify code and configuration on any MBCP Resource, unless directed to do so by authorized personnel.

All Users are responsible for safeguarding Sensitive Information. Users may access, use or share Sensitive Information held by MBCP only to the extent it is authorized and necessary to fulfill their assigned job duties. Users must immediately notify IT Support if Sensitive Information is inappropriately shared or exposed.

Users must immediately report to IT Support any suspicious e- mail or other computer activity.

D. NO EXPECTATION OF PRIVACY

MBCP owns all Data stored on Agency Resources and reserves the right to access anything the User has viewed or created using those Resources.

Users shall have no expectation of privacy. Authorized MBCP staff may view any and all activities and Data created, stored or transmitted using MBCP Resources. They may access any electronic Data or files at any time without consent from or notification to the User.

MBCP may monitor, record and review any Data or websites a User may have accessed through an MBCP internet connection.

MBCP strongly discourages the storage of personal files and messages (pictures, personal email, texts, instant messages, music, spreadsheets, etc.) on MBCP-provided computers. All such Data may be accessed and reviewed at the Agency's discretion and may be deleted without notice.

E. HARDWARE AND SOFTWARE CONTROL

- Alteration, upgrade, or modification to computer equipment, software program, IT facilities is prohibited without IT approval.
- No software installation is allowed by a user without IT approval.
- User is not allowed to attach any non-company issued or unauthorized device, such as a USB storage device, printer or video cam, to the company's computer equipment, network equipment, or other IT assets. This restriction includes the unauthorized installation of any additional network-related or digital communications equipment such as routers, network switches or wireless access points.
- The company retains ownership of all company-owned hardware and software programs provided to users. The Company is not responsible for any computer equipment that is not provided by the Company.
- User is responsible for taking all reasonable safety precautions with mobile devices (laptops and mobile phones) to protect them from theft or physical damage.
- User must report to his/her supervisor and IT Support, as soon as possible, in the event of any computer equipment loss.

F. RESTITUTION

Should a user fail to return MBCP-provided computer equipment upon termination, the company reserves the right to ask the user to pay the current market value of the equipment as determined by the CEO.

V. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

The Internal Operations Department 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.

B. NON-COMPLIANCE

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

IT3
Category: INFORMATION TECHNOLOGY

E-MAIL USE POLICY

I. PURPOSE

The purpose of this policy is to ensure the proper use of MBCP's E- mail system and make users aware of what the Agency deems as acceptable and unacceptable use of its E-mail system. This policy outlines the minimum requirements for use of E-mail within the MBCP Network.

It is the responsibility of all E-mail users to understand and comply with this policy. These guidelines are intended to provide MBCP employees with general examples of acceptable and unacceptable uses of MBCP's E-mail system.

II. SCOPE

This policy covers appropriate use of any E-mail sent from a MBCP E-mail address and applies to all employees, vendors, and agents operating on behalf of MBCP.

III. BACKGROUND

In the past decade, there has been an explosion in the use of electronic communication, and email is at the forefront of this. With increased usage come many risks, especially for a public agency. These include threats of confidentiality leaks (e.g. of sensitive information), legal liabilities (e.g. disparaging comments about customers), and misconduct (e.g. sending of racist jokes). Email policies are therefore an important guide for employees to understand what is appropriate, and inappropriate use of MBCP's email accounts. The remainder of this policy document outlines some specific policy and process guidelines which should be followed at all times.

IV. DEFINTIONS

"Chain E-mail or Letter" refers to E-mail sent to successive people.

“E-mail” refers to the electronic transmission of information through a mail protocol such as SMTP or IMAP. MBCP’s typical E-mail client is Microsoft Outlook.

“Forwarded E-mail” refers to an E-mail message resent from an internal network to an outside address.

“Sensitive Information” includes all data, in its original and duplicate form, which contains personal information, protected health information, customer record information, card holder data, confidential personal data, or information that is deemed to be confidential or is otherwise exempt from disclosure under state law.

“Unauthorized Disclosure” refers to the intentional or unintentional revealing of Sensitive Information to people, whether inside or outside of MBCP, who do not need to know that information.

IV. POLICY

A. BUSINESS PURPOSE

This E-mail policy governs the use of MBCP’s E-mail system at any location and using any device, MBCP-provided or other.

All use of E-mail must be consistent with MBCP policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

MBCP E-mail account should be used primarily for MBCP business-related purposes; personal communication is permitted on a limited basis, but non-MBCP related commercial uses are prohibited.

The MBCP E-mail system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any E-mails with this content from any MBCP employee should report the matter to their supervisor immediately.

Employees are prohibited from using MBCP resources to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for a religious or other personal cause.

E-mail signatures, if used, shall only include business-related information such as name, title, MBCP contact information, MBCP logo, links to MBCP websites and/or social media accounts, and MBCP-related messages.

B. PERSONAL E-MAIL ACCOUNTS

Incidental use of MBCP resources (computers and networks) for accessing personal E-mail accounts is acceptable but only via web browser (e.g. www.gmail.com, etc.)

Employees may not configure auto-forwarding of MBCP E-mail to external E-mail accounts.

Employees may not use personal E-mail accounts or text messages to conduct official MBCP business.

Users are prohibited from using third-party E-mail systems and storage servers such as Google, etc. to conduct MBCP business, to create or memorialize any binding transactions, or to store or retain E-mail on behalf of MBCP. Such communications and transactions should be conducted through proper channels using MBCP approved documentation.

C. ACCESSING MBCP E-MAIL ON PERSONAL DEVICES

Any employee who connects to or stores MBCP work E-mail on his/her personal device is responsible for safeguarding access to his/her MBCP mailbox. Any such device used by the employee must be owned by the employee.

Access to an MBCP E-mail account must be under user control always. The employee is responsible for all E-mails sent out from his/her account whether or not s/he intended the E-mail to be sent. The employee is required to maintain a passcode to lock the device for as long as MBCP work E-mail is accessible from the device.

In the event the device is lost or stolen, the employee is required to change (or arrange to have changed) his/her network/E-mail password and any others that may be compromised as soon as possible and no more than 24 hours after the discovery of the theft or loss.

MBCP, its employees, directors and management staff are not liable for loss of personal information, files, etc. stored on employee's personal device as a result of access to MBCP's E- mail system.

D. PASSWORDS

E-mail passwords are the property of MBCP. Only specific MBCP approved personnel are authorized to access another employee's E-mail. Misuse of passwords, sharing of passwords with others, and/or the unauthorized use of another employee's password will result in disciplinary action, up to and including termination.

E. SENSITIVE DATA

Wherever possible, sensitive data should not be transferred via email as email is not generally encrypted or password protected. To minimize the sensitive data loss via email communications, sensitive information should not be included in the body of an email. *Best Practice: It is recommended that sensitive information be transferred in a document (e.g. MS Word, MS Excel), with password protection. When notifying the password to the authorized person for opening that document, the password should not be in the same email with the password protected document.*

F. NO EXPECTATION OF PRIVACY

All communications and information that pass through the MBCP computer systems, including E-mail, belong to the Agency. The federal Electronic Communications Privacy Act of 1986 gives management the right to access and disclose all employee E- mail messages transmitted or received via the organization's computer system. When it comes to E-mail, employees should have no expectation of privacy. MBCP reserves the right to access and monitor E-mail at any time for any reason without notice, and may disclose E-mail to regulators, courts, law enforcement agencies, and other third parties without the employee's knowledge or consent.

G. OFFENSIVE CONTENT AND HARASSING OR DISCRIMINATORY ACTIVITIES ARE PROHIBITED

Messages containing defamatory, obscene, menacing, threatening, offensive, harassing, or otherwise objectionable and/or inappropriate statements—and/or messages that disclose personal information without authorization—are prohibited. If you receive this type of prohibited, unsolicited message, do not forward it. Notify your supervisor and/or HR Manager about the message.

H. BUSINESS RECORD RETENTION

E-mail messages are written business records and are subject to laws and policies for retaining and destruction of business records. Refer to P&P AD4 - Records Retention Policy for details.

I. PHISHING

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity (e.g. another company or a government agency) in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure unsuspecting users. Phishing emails may also contain links to websites that are infected with malware (software that harms your computer or enables extraction of information from your computer). Phishing often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

If you receive any such emails that you feel have any suspicious or potentially fraudulent content, do not reply or click on any links on the e-mail and notify IT Support immediately for further instructions.

J. EMAIL MANAGEMENT, RETENTION AND ARCHIVING

As a best practice, employees should be aware of the importance of proper email management, retention and archiving practices, and consider issues including basic individual organization, emails as legal records, and physical storage space. Defining a management, retention and archiving policy is a balance of all of these considerations. The policy below provides guidelines on the management of email.

Emails typically fall into two main types – transitory and retainable:

1. Transitory Emails

Transitory emails do not set policy, establish guidelines or procedures, certify transactions, confirm major decisions, or become a receipt. They convey information of a temporary importance. Examples include:

- Telephone messages
- Invitations and responses to invitations

- Thank yous
- Replies to routine questions
- Spam or unsolicited emails

Transitory emails are the most prevalent in our day-to-day work and should be the ones most regularly cleaned up (i.e.. deleted).

2. Retainable Records

Emails that are informational, related to decision making, received in connection with a transaction, or are otherwise seen as having referable importance in the future may be considered as retainable records. Examples include:

- Activity reports
- Audit trail reports
- Management reports
- Project work plans
- Status reports
- Requests for information or action
- Statements of policy
- Documentation of oral exchanges from meetings or telephone calls during which business was discussed, policy formulated or decisions taken

Retainable Records should be filed and/or archived according to P&P AD4 – Records Retention Policy.

Each employee is responsible for managing all sent and received emails. This refers to the sorting, filing and retaining or deleting of emails. Generally speaking, good basic "housekeeping" of emails includes:

- General organization (e.g. use of folders)
- Periodic purging of personal emails (especially those with large attachments)
- Retention of those that are work related
- Detaching of large but important attachments to your PC (in both received and sent emails)
- Use of the archiving function in your email software (where available)

The larger your email account, the slower it will be and the harder it is to find things. MBCP resources also need to be increased as more and more email data is stored.

V. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

The Internal Operations Department 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.

B. NON-COMPLIANCE

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

IT4
Category: INFORMATION TECHNOLOGY

IT ASSET MANAGEMENT POLICY

I. PURPOSE

The purpose of the IT Asset Management Policy is to provide a record of valuable IT assets for tracking and accounting purposes in order to enable management to allocate IT resources, and plan IT developments to meet MBCP's requirements and changes.

II. SCOPE

This procedure applies to all MBCP's IT assets.

III. DEFINTIONS

"Information Technology (IT) Asset" refers to any computer hardware, software, Information Technology-based MBCP information, related documentation, licenses, contracts or other agreements, etc. In this context, "asset" and "Information Technology (IT) Asset" are understood to be the same.

IV. ASSETS TRACKED

This section defines what IT assets should be tracked and to what extent they should be tracked, categorized below are the types of assets subject to tracking:

- Computer systems -Laptops and desktops
- Printers, Copiers, Monitors, Multifunction Machines
- Handheld devices (iPads and Tablets, etc.)
- High Value Hardware (Switches, Firewalls, Servers, etc.)
- AV systems
- Desk Phones and Speaker Phones
- Software, including
    - Software license or certificate, if applicable

- Expiry date for license or certificate, if applicable

It is not mandatory to record the following items in the IT asset inventory:

- Mouse
- Keyboard
-
- Cables (Network, Power, Monitor, etc.)
- Low Value Hardware (Headsets, Laptop Locks, etc.)

V. POLICY

1.0 IT ASSET BUDGET AND PLANNING

1.1 The Internal Operations Department is responsible for planning upgrades and replacements of the hardware and software.

1.2 It is suggested that hardware upgrades or replacements are considered when the hardware is approaching 4-5 years old.

2.0 IT ASSET INVENTORY

- An IT asset inventory must be maintained by IT Support to register and manage all IT hardware and software. The objectives of this inventory are to provide full detailed information of all hardware and software, and its allocation by user or department / location. Also, IT Support can use this inventory to plan the reallocation of IT assets to maximize existing resources.
- The IT Support is responsible for managing the IT asset inventory, maintaining its accuracy and ensuring that it is up to date.
- For IT hardware, the IT asset inventory must include the following information:
    - User or system name for server equipment
    - Location
    - Brand and model
    - Specifications (example : CPU, memory, hard disk size, operating system)
    - Serial number
    - Inventory Code
    - Invoice date (MMYYYY or YYYY)
    - Purchased price
    - Expected replacement date corresponding with warranty expiration or end of useful life

- For IT software, the following information must be registered in the IT Asset inventory Register:
    - Software and version
    - Total number of licenses per software
    - Subscription expiration if applicable
- What employee or asset to which the software license is assignedExamples of purchased IT software are:
    - Windows server license
    - Microsoft client access license
    - Microsoft Office
    - Antivirus
    - Expected Write Off Period / Replacement Date if aplicable
- All IT assets are required to be labeled with the assigned Inventory code.

2.1 IT ASSET INVENTORY REVIEW

- The objectives of the review are to:
    - Verify the hardware and software information in the asset inventory
    - Check whether any IT assets have been lost
    - Check whether any unauthorized software has been installed
    - Update the asset inventory for any discrepancies
- The IT asset inventory must be reviewed by IT Support at least once a year, preferably before the annual budget time so that the inventory reflects the latest status for budgeting and planning.
- A review of the IT asset inventory must be signed off by IT Support to ensure that the inventory is accurate and up to date.
- If mobile devices cannot be checked physically by the IT department during the review, it is acceptable for users to sign off to confirm that the devices are still available and in working condition.
- If any illegal, unlicensed or unauthorized software is found during the review, it must be removed immediately.

3.0 IT ASSET ACQUISITION

3.1 MBCP personnel shall use the Purchase Requisition Form (refer to P&P FP8 Purchasing and Procurement Policy) to request new IT Assets. This form shall be approved by the

appropriate approval matrix established at the Purchasing and Procurement Policy before being submitted to IT Support.

3.2 If a purchase or lease agreement exists for the kind of asset being requested, that asset shall be ordered from the existing vendor, pursuant to the terms of the agreement.

- If such an agreement does not exist, IT Support may recommend entering into one.

4.0 IT ASSET INSPECTION, ACCEPTANCE & DISTRIBUTION

4.1 Physical assets shall be received by the Administrative Assistant and forwarded to IT Support, or directly by the IT Support.

- IT Support may receive non-physical assets, such as application software, directly from the vendor.

4.2 IT Support shall inspect and test assets for performance and capability prior to acceptance, if possible.

- IT Support shall contact the vendor for replacement of the nonconforming asset and dispose of or return the nonconforming asset in accordance with any purchase/lease agreement in place.

4.3 All assets must have an ID number. Either an internal tracking number will be assigned when the asset is acquired or the use of Manufacturer ID numbers.

- An asset tracking database shall be created to track assets.
- When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset tracking database.

4.4 IT Support shall forward the packing slip or invoice to Finance for payment.

4.5 Only IT Support shall distribute and install IT Assets.

- In the case of assets designed for use by individuals, installation shall be scheduled primarily for the user's convenience.
- In the case of assets used by multiple individuals (network hardware/software, operating systems, common application software, etc.):
    a. Installations shall be scheduled at a date and time that will affect the least number of users;
    b. Ample advance notice shall be given to affected users; and
    c. IT Support shall mitigate risk by ensuring backup and/or redundancy of the affected systems/applications.

4.6 IT Support shall update the IT Asset Inventory Register after installing assets.

5.0 IT ASSET TRANSFER

The following actions shall be considered when a computer device will be transferred to another user:

5.1 IT Support should verify the transferring of equipment to a new user follows all asset tracking guidelines and does not allow access to a previous user's data.

- If a used device is transferred to another user, all the previous user's data, cookies, files and personal preferences must be removed from the device to prevent unauthorized access and/or the leakage of any personal information. It is recommended that the device is reset to the factory or MBCP's default for each user.
- Software that is not required by the next user should be removed and its license returned to the IT asset inventory.
- Hardware and software will be installed as per next user's requirements.
- The IT asset inventory must be updated in accordance with any changes.

6.0 IT ASSET DISPOSAL

6.1 IT Support should notify Finance to write off any equipment planned for disposal by completing the Fixed Asset Transfer/Disposal Request Form.

6.2 When technology assets have reached the end of their useful life, they should be given to IT Support for proper disposal. Acceptable methods for the disposal of IT assets are as follows:

- Sale to staff
- Donation to charities, non-profit organizations, schools, etc.
- Sale as scrap to a licensed dealer
- Use as a trade-in against the cost of a replacement
- Reassignment to a less critical business operation function
- Recycling

6.3 This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within MBCP.

6.4 All IT Assets shall be disposed of in accordance with the following disposal policy:

a. Asset disposal is a special case since some assets might have sensitive data on it. MBCP's disposal policy will mandate that all assets that contain data will have the disks wiped using disk destruction software. The data must be erased using an approved technology to make sure it is not readable using specialized data retrieval techniques. The following asset types will be checked for wipe:

- Memory stick
- CD ROM disk Storage tape
- Mobile device (e.g. tablet, mobile phone, etc.)
- Hard drive

b. Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

c. IT Support is responsible for decommissioning this equipment by:

- Deleting all data files
- Removing a web browser's cookies
- Removing any saved log in and / or passwords from the web browser
- Removing the browser's history
- Uninstalling licensed programs and / or applications

6.5 IT Support will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and initials of the technician who performed the disk wipe.

6.6 No computer equipment should be disposed of via dumps, landfill, etc. IT Support will properly remove all data prior to final disposal. Final disposal will be processed through a certified e-waste recycle vendor.

6.7 Upon disposal of said assets, IT Support shall update the IT asset inventory.

7.0 LOST OR STOLEN IT ASSETS

If any IT equipment is lost or stolen, the user must inform IT Support and/or all relevant parties (e.g. his/her direct supervisor) immediately of the following:

- Username
- Contact number of the user
- Any potentially sensitive data stored on the device
- Time the device was lost
- Location where the device was lost
- Reason for loss (example: theft, misplacement)

- The user is required to report any loss/theft of equipment to the police and obtain a police report to support the incident.
- IT Support will notify Finance of the loss / theft so that they can write it off. IT Support should also update the IT asset inventory immediately to reflect the changes.

- MBCP reserves the right to ask the user to pay the current market value of the lost/stolen equipment, as determined by the CEO.

VI. POLICY COMPLIANCE

A. COMPLIANCE

The Internal Operations Department 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.

B. NON-COMPLIANCE

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

ATTACHMENT:

1. Fixed Asset Transfer/Disposal Request Form

Monterey Bay Community Power

Local Choice • Clean Energy • Economic Vitality
MBCommunityPower.org

FIXED ASSET TRANSFER/DISPOSAL REQUEST FORM

Date: _____

Description of asset: _____

Years since purchase: _____

Quantity: _____

Justification for disposal: _____

(Please attach further information for consideration, if necessary)

Gain / Loss on disposal

Original Cost:

Accumulated Depreciation: _____

Net Book Value: -

Claims from insurer: _____

Gain / (loss) on disposal: _____

REQUESTED BY

_____

APPROVED BY

_____
Director of Internal Operations

APPROVED BY

_____
CEO
(Disposal > $5,000)

IT5
Category: INFORMATION TECHNOLOGY

INTERNET USAGE POLICY

I. PURPOSE

Provide MBCP staff with rules and guidelines about the appropriate use of network and Internet access. Having such a policy in place helps to protect both the business and the employee; the employee will be aware that browsing certain sites or downloading files is prohibited and that the policy must be adhered to, thus leading to fewer security risks for the business as a result of employee negligence.

II. SCOPE

All users of MBCP's network/internet infrastructure.

III. DEFINITIONS

"Information Systems" refers to all resources that store, transmit or present information related to MBCP business

"Resources" refers to all MBCP-owned hardware and software including, but not limited to:

- Computers, laptops, tablets, phones
- Monitors, printers, scanners,
- Network storage, network infrastructure, servers
- All software applications licensed by MBCP
- Accounts such as email account or other accounts used to access MBCP applications
- Data plans, subscription services
- Audio and video equipment

IV. POLICY

A. ACCEPTABLE USE

- This Internet Usage Policy applies to all employees of MBCP who have access to computers and the Internet to be used in the performance of their work. Use of the Internet by employees of MBCP is permitted and encouraged where such use supports the goals and objectives of the business. However, access to the Internet through MBCP is a privilege and all employees must adhere to the policies concerning Computer, Email and Internet usage. Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment. Employees may also be held personally liable for damages caused by any violations of this policy.

- Company employees are expected to use the Internet responsibly and productively.

- All Internet data that is composed, transmitted and/or received by MBCP computer systems belongsto MBCP and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

- The equipment, services and technology used to access the Internet are the property of MBCP and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections.

- All sites and downloads may be monitored and/or blocked by MBCP if they are deemed to be harmful and/or not productive to business.

B. STRICTLY PROHIBITED USE

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet;

- Using an unauthorized VPN or other encryption/usage masking service;
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy;

- Stealing, using, or disclosing someone else's password without authorization;

- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization;

- Sharing confidential material, trade secrets, or proprietary information outside of the organization;

- Hacking into unauthorized websites;

- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers; or

- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems.

IV. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

The Internal Operations Department 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.

B. NON-COMPLIANCE

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

IT6
Category: INFORMATION TECHNOLOGY

IT ACCESS CONTROL POLICY

I. PURPOSE

To prevent unauthorized access to or use of MBCP information, to ensure its security, integrity, and availability to appropriate parties.

II. SCOPE

This applies to all MBCP information and to all storage and access methods.

III. DEFINITIONS

"Access Control" refers to enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access (or, providing access to authorized users while denying access to unauthorized users).

IV. POLICY

A. BUSINESS REQUIREMENTS FOR REGULATING ACCESS

Every Information Technology (IT) user shall have a unique identifier and a system password assigned.

There shall be a system in place for authenticating and authorizing users beyond the login point. Access to applications, databases, etc., once a person is in the system must be controlled.

Each user shall be given access to IT resources based on position and department.

User activity shall be monitored frequently and reviewed for unusual, unauthorized or illegal activity, current periods of inactivity, etc. User access may be suspended for, but to limited to, the following:

- A number of consecutive failed log-on attempts;
- Unauthorized or illegal activity; or
- An extended period of account inactivity.

B. MANAGEMENT OF USER ACCESS

Users shall be formally registered at the time of their employment with MBCP. Users shall be re-registered upon changing jobs within MBCP and deleted/un-registered upon leaving MBCP.

Access to MBCP information shall be granted on a need-to-know basis. Users shall be authorized according to their duties. Access may be “read only”, “read/write”, or “full access” and users may or may not be given administrative privileges for their computers and for certain data.

Additional access may be requested and will be addressed based on a two-step verification process. IT personnel will obtain authorization from both the manager of the department holding the requested data and the Director of Internal Operations. A supporting reason along with a specific business need will be required before authorization for access is given.

Password Control – refer to P&P IT7 Login and Password Security Policy for details.

IT Support shall review all users’ access rights/privileges on a regular basis.

C. USER RESPONSIBILITIES

- Users must secure their equipment if it is to be unattended for any length of time. Screen locks should automatically activate after 10 minutes of inactivity (users may set screen locks to activate sooner and they should be allowed to activate screen locks immediately, if desired).

- Users shall have direct access only to services and information that they have been specifically authorized to use. IT Support shall maintain an access control database for that purpose.

D. OPERATING SYSTEM ACCESS CONTROL

- Access to a local operating system shall be limited to authorized users (for example, the assigned employee)
- Access to remote operating systems shall be limited to authorized users (for example, IT Support staff).

- Only authorized support personnel shall be authorized to access remote operating systems and utilities outside of normal business hours.

- Access to remote and local operating systems and related utilities shall be logged and such logs shall be reviewed periodically by IT Support.

- Remote Operating systems connections shall be terminated after 15 minutes of inactivity.

E. MONITORING SYSTEM ACCESS USE

- Instances of access and use of any IT resource shall be automatically logged.

- Access control logs shall be retained in accordance with legal and regulatory requirements.

IV. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

The Internal Operations Department 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.

B. NON-COMPLIANCE

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

IT7
Category: INFORMATION TECHNOLOGY

LOGIN AND PASSWORD SECURITY POLICY

I. PURPOSE

The purpose of this policy is to promote a secure computing environment throughout MBCP's network by establishing standards for managing login accounts and strengthening password security.

II. SCOPE

This policy is applicable to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any MBCP facility, has access to the MBCP network, resides on third party servers (Office 365, etc), or stores any non-public MBCP information.

-III. POLICY

Where technically and operationally feasible, the following account and password management practices must be followed:

A. PASSWORD CREATION AND PASSWORD CHANGE

a. A password is required for all login accounts. All user passwords must conform to the Password Construction Guidelines is in Attachment 1.
b. First time password change is enabled for the initial login by the user.
c. Password is changeable by user.
d. Password must be changed at least every 90 days.

e. A new password cannot be the same as any of the last four used for that account.
f. Password cracking or guessing may be performed on a periodic or random basis by the IT Support Team. If a password is guessed or cracked during one of these scans, the user will be required to change it.
g.

B. PASSWORD PROTECTION

a. The login account is unique and is assigned to an individual user. A login account cannot be shared.
b. If an administrator password is required by a supplier for troubleshooting or an upgrade, IT Support will not disclose the password but must input it to the required system himself/herself. If a password is disclosed, IT Support must change it as soon as possible.
c. An administrator-level account cannot be shared. Multiple administrator accounts are required for multiple administrator-level personnel.
d. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential MBCP information.
e. Do not reveal a password on questionnaires or security forms.
f. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile device (phone, tablet) without encryption.
g. Any user suspecting that their password may have been compromised must report the incident to IT Support and change all passwords.

IV. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

The Internal Operations Department 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.

B. NON-COMPLIANCE

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

V. ATTACHMENT:

1. Password Construction Guidelines

PASSWORD CONSTRUCTION GUIDELINES

OVERVIEW

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data or the MBCP network. This guideline provides best practices for creating secure passwords.

SCOPE

This guideline applies to employees, contractors, consultants, temporary and other workers at MBCP. This guideline applies to all passwords including but not limited to user-level accounts, system- level accounts, web accounts, e-mail accounts, screen saver protection and voicemail.

STATEMENT OF GUIDELINES

All passwords should meet or exceed the following guidelines:

STRONG PASSWORDS HAVE THE FOLLOWING CHARACTERISTICS:

- Contain at least 12 alphanumeric characters.
- Contain both upper and lower-case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, #$?!).

POOR, OR WEAK, PASSWORDS HAVE THE FOLLOWING CHARACTERISTICS:

- Contain at least eight characters.
- Can be found in a dictionary or exists in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone number, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, 123321, etc.
- Are some version of “Welcome123”, “Password123”, etc.

- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).

PASSPHRASES

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines and include upper and lower case letters, number, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

IT8
Category: INFORMATION TECHNOLOGY

DATA BREACH RESPONSE POLICY

I. PURPOSE

The purpose of the policy is to establish the response to a data breach. This policy will clearly define Data Breach, to whom it applies and under what circumstances, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

MBCP Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how MBCP's established culture of openness, trust and integrity should respond to such activity. SVCE Information Security is committed to protecting MBCP's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

II. SCOPE

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of MBCP customers, employees, and protected information of suppliers.

III. DEFINITIONS

“Encryption or encrypted data” – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text.

“Plain text” – Unencrypted data.

“Hacker” – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

“Protected Health Information (PHI)” - Any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

“Personally Identifiable Information (PII)” - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data.

“Protected data” - See PII and PHI.

“Information Resource” - The data and information assets of an organization, department or unit.

“Safeguards” - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

“Sensitive data” - Data that is encrypted or in plain text and contains PII or PHI data (see PII and PHI above).

IV. POLICY

A. GENERAL

As soon as a theft, data breach or exposure containing MBCP's Protected data or MBCP's Sensitive data is identified, the process of removing all access to that resource will begin.

The CEO will be notified of the theft, breach or exposure and IT personnel will immediately change all passwords on the effected platform (e.g. Firewall, Email Infrastructure, File Shares, etc.).

The CEO will chair an incident response team to handle the breach or exposure. The team will include members from:

- Internal Operations;
- IT Supports;
- Communications and External Affairs;
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed;
- Additional departments based on the data type involved;
- Additional individuals as deemed necessary by the CEO.

IT Support, along with the designated team, will analyze the breach or exposure to determine the root cause. After the cause is determined IT personnel will take appropriate security measures to mitigate a future occurrence.

B. DEVELOP A COMMUNICATION PLAN

The incident response team will decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

IV. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

The Internal Operations Department 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.

B. NON-COMPLIANCE

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

IT9
Category: INFORMATION TECHNOLOGY

WORKSTATION SECURITY (FOR HIPAA) POLICY

I. PURPOSE

The purpose of this policy is to provide guidance for workstation security and to ensure the requirements of HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

II. SCOPE

This policy applies to all MBCP employees, contractors, vendors and agents with an MBCP-owned or personal workstation connected to the MBCP network.

III. POLICY

A. GENERAL

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and access to sensitive information, included protected health information (PHI), is restricted to authorized users.

MBCP will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Appropriate measures include:

- Securing file cabinets to restrict physical access to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with the P&P IT7 Login and Password Security Policy.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, including PHI on network servers.

- Keeping food and drink away from workstations in order to avoid accidental spills.
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Exiting running applications and closing open documents after use.
- Ensuring all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- Securing laptops that contain sensitive information by using cable locks or locking laptops in drawers or cabinets.

IV. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

The Internal Operations Department 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.

B. NON-COMPLIANCE

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

IT10
Category: INFORMATION TECHNOLOGY

CLEAN DESK POLICY

I. PURPOSE

The purpose of this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive information about employees, MBCP intellectual property, customers and vendors is secure in locked areas and out of sight.
A Clean Desk policy is not only ISO 27001/17799 Information Security Management compliant, but it is also part of standard basic privacy control.

II. SCOPE

This policy applies to all MBCP employees and affiliates.

III. POLICY

- Employees are required to ensure all sensitive/confidential information in hardcopy or electronic format is secure in theirwork area at the end of the day and when they are expected to be gone for an extended period of time.
- Computer workstation screens must be locked when workspace is unoccupied.
- Any restricted or sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing restricted or sensitive information must be kept closed and locked when in use or when not attended.
- Keys used for access to restricted or sensitive information must not be left at an unattended desk.

- Portable computing devices (including laptops and tablets) must be either locked with a locking cable or locked away in a drawer when away from office for a period of time.

- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

- Printouts containing restricted or sensitive information should be immediately removed from the printer.

- Upon disposal, restricted or sensitive documents should be shredded in the official shredder bin.

- Whiteboards containing restricted and/or sensitive information should be erased.

- Mass storage devices such as USB drives should be treated as sensitive information and be secured in a locked drawer.

- All printers should be cleared of papers as soon as they are printed; this helps ensure sensitive documents are not left in printer trays for the wrong person to pick up.

IV. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

The Internal Operations Department 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.

B. NON-COMPLIANCE

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

IT11
Category: INFORMATION TECHNOLOGY

THREAT RISK ASSESSMENT

I. PURPOSE

MBCP shall regularly evaluate its Information Technology (IT) systems and network for threats and vulnerabilities in order to protect its IT assets and reduce the risk to MBCP.

II. SCOPE

This procedure applies to all of MBCP's IT assets, including the IT network.

III. DEFINITIONS

Risk – Possibility of losing availability, integrity, or confidentiality of IT assets due to a specific threat; also, the product of threat level and vulnerability level.

Threat – Expression of intent to inflict injury, damage or potential violation of security.

Threat Assessment – A process by which types of threats an IT network might be vulnerable to and where the network is most vulnerable are identified.

Vulnerability – Flaw or weakness in a system's design, implementation, or operation and management that could be exploited.

IV. POLICY

A. IT THREAT & RISK ASSESSMENT – INTRODUCTION

In order to prepare for Threats to its IT assets and infrastructure, MBCP must be aware of the types of Threats that exist, the likelihood that they will occur, their potential impact, and the Risk these Threats may pose.

Threats may be natural or manmade. Natural Threats include floods, storms, and earthquakes. Manmade Threats may be accidental or intentional. Examples of manmade

Threats include use of unauthorized hardware or software and having unauthorized access to MBCP systems.

Intentional Threats exist both outside the Agency and within.

The Risk posed by any given Threat is a function of the combined likelihood of the Threat occurring and the impact it would have on MBCP's assets (hardware, software, data, network/infrastructure, and personnel) if it were to occur. While Risk to MBCP's IT assets cannot be completely eliminated, the Agency must make all reasonable efforts to minimize Risk. Those efforts should begin with assessing Threats and Risks.

B. IT THREAT ASSESSMENT PREPARATION

In advance of conducting a Threat Assessment of any of MBCP's IT systems, IT Support shall establish a baseline for assessment, identifying systems to be assessed (power supply, HR, marketing, etc.) and determining their interconnectivity with other systems.

IT Support should identify and describe Threats that may target the IT assets and systems under consideration by one or more of the following means:

- Periodically reviewing Access Control Log for threat occurrences, such as unauthorized system access.
- Reviewing IT incidents for trends and/or patterns.
- Reviewing any system test (test script, test procedures, expected results, etc.) for vulnerabilities testing.
- Conducting penetration testing at irregular intervals, to verify the IT network's ability to withstand intentional attempts at circumventing IT security.

IT Support may acquire additional information for developing the assessment baseline by routinely reviewing Threat alerts and bulletins from vendors, standards organizations, etc.

To determine if MBCP needs to act on any given Threat and to what extent it should act, IT Support shall classify the likelihood of Threats/ Vulnerabilities in the following manner:

- Low – the Threat is unlikely to occur;
- Medium – the Threat may occur. For example, MBCP is located in an earthquake zone, so an earthquake is likely to have an effect on MBCP;

- High – the Threat is likely to occur. For example, if MBCP does not require password access to computers or data stores, the likelihood is high that someone will eventually access and steal or compromise MBCP data.

To determine if MBCP needs to act on any given Threat and to what extent it should act, IT Support shall classify the impact of Threats/ Vulnerabilities in the following manner:

- Low – the Threat may result in minimal loss of MBCP assets/resources;
- Medium – the Threat may result in a significant loss of MBCP assets/ resources, harm MBCP's mission or interests, or result in injury to an employee;
- High – the Threat may result in a very costly loss of MBCP's assets/resources, significantly harm MBCP's mission, interests, or standing, or result in serious or fatal injury to an employee.

An exposure rating or Risk assessment shall be based on likelihood and impact ratings. A Risk matrix is prescribed (Figure 1), with likelihood running from low to high along one axis and impact running from low to high on the other axis.

	Impact	Low	Medium	High
Likelihood	High	Low	Medium	High
	Medium	Low	Medium	Medium
	Low	Low	Low	Low

FIGURE 1 – RISK MATRIX

The resulting exposure rating/Risk assessment shall be used to prioritize Threats (Figure 2).

- High-risk Threats require the highest security levels and present the greatest need for immediate action, if existing security tools and techniques are inadequate.
- Medium-risk Threats require a response to be scheduled for implementation within a reasonable timeframe.
- Low-risk Threats may require little or no response on the part of the IT Support.

Risk Level	Description and Actions
High	Preventive actions are required and a preventive action plan shall be developed and implemented as soon as possible.
Medium	Preventive actions are required and a plan to incorporate those actions within a reasonable time frame shall be developed.
Low	IT Support should confer with managers of affected systems to determine if preventive action is required or if risk is acceptable.

FIGURE 2 – THREAT PRIORITY

C. IT THREAT/RISK ASSESSMENT

At regular intervals, IT Support shall conduct a Threat/Vulnerability assessment of the IT network. IT Support shall review the results and analyze the findings in order to determine if action is required and to what extent.

D. IT THREAT/RISK REVIEW

IT Support shall periodically review the Risk assessment process to ensure its continued timeliness and applicability. Historical data (i.e., number, nature, and severity of Threats over time) shall help determine if Risks are under control.

Any time a significant implementation, revision, etc., takes place, IT Support shall review the Risk assessment process, to ensure existing controls are applicable to such changes or if improved controls are required.

V. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

The Internal Operations Department 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.

B. NON-COMPLIANCE

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

IT12
Category: INFORMATION TECHNOLOGY

MALWARE DEFENSE POLICY

I. PURPOSE

The purpose of this policy is to prevent data loss, corruption, or misuse of MBCP computing resources or information that may occur when malware is introduced to MBCP's IT network.

II. SCOPE

This policy applies to all MBCP personnel and to all computer hardware and software comprising MBCP's IT network.

III. DEFINITIONS

Malware - Short for "malicious software", malware is designed to damage, disrupt, or abuse an individual computer or an entire network and/or steal or corrupt an organization's most valuable and sensitive data. Viruses, worms, and Trojan horses are examples of malware.

Spam or junk email – Unsolicited commercial email sent in bulk over the Internet. Spam puts a cost and a burden on recipients by clogging up network bandwidth, consuming disk space, and wasting employees' time. Spam is frequently a malware vector.

Subscription service – A service whereby a software vendor offers support for its product, usually for a predetermined time period. Anti-virus vendors typically include a one-year subscription (for updates, notices, etc.) with the purchase of a product license. Many vendors offer fee-based subscription services whereby subscribers automatically receive notifications, security bulletins, etc., for a set period of time.

Target – The ultimate destination for Malware; that which the malware is designed to attack. Boot sectors, hard disk drives, email servers, and departmental (HR, accounting, etc.) servers are examples of malware targets.

Vector – How malware is carried to a computer, server, or system.

IV. POLICY

A. MALWARE DEFENSE PLANNING

Malware is commonly passed to a potential Target through email. The person who receives the email opens an attachment, which unleashes the Malware, which then spreads to other computers via a shared network (Malware may attack by other means, but this is a common method). To lessen the potential for damage to MBCP's Information Technology (IT) assets by Malware, the Agency shall develop and implement a multifaceted approach to Malware prevention.

To prepare MBCP's Malware Defense Plan, IT Support shall review the following items:

- Asset Inventory Database
- IT industry standards and best practices
- Anti-Malware vendor websites or portals
- IT security alerts and bulletins (many of which are available for free and as a subscription service).

B. MALWARE DEFENSE PLAN

IT Support shall install firewalls on all personal computer (PC) workstations and on all servers.

IT Support shall ensure that operating systems, web browsers, email programs, and related software are configured for optimum security.

IT Support shall install an anti-virus program on every PC and server and all anti-virus software shall be automatically updated using a subscription service (updates should be automatically logged by the software).

All anti-malware protections shall be configured to prevent being disabled by users. Only IT Support shall be allowed to temporarily disable anti-malware measures (for example, disabling a local antivirus program to install and configure an application locally).

MBCP shall minimize malware risks by backing up critical information.

C. MALWARE DEFENSE PLAN REVIEW

IT Support shall periodically review all anti-virus, firewall, and other relevant logs to determine if the software is up-to-date and is performing as expected.

D. MALWARE DEFENSE PLAN UPDATE

IT Support shall incorporate updates into the Malware Defense Plan as needed to address the latest trends in malware defense.

E. CONTAINMENT

Once a malware threat has been carefully analyzed it needs to be effectively contained so that the infection will not continue to spread. IT will develop a strategy to halt malware propagation. Once the strategy has been outlined the procedures to contain the malware threat should be followed quickly and efficiently. Procedures to contain the threat may include (but are not limited to):

- Disable physical network access
- Disable network services: To shutdown network services it will likely be necessary to modify host, server, or network firewalls, and network routing device
- Host, service, and application hardening -Vulnerable systems should be protected by applying service, application, and operating system patches as necessary
- Power off infected systems

F. ERADICATION

After analysis and containment of a malware outbreak the threat needs to be removed from all infected hosts.

- Scan with installed antivirus software (make sure current definitions are installed)
- Restore from backup media (use system restore, wipe drive, full format)
- Reload operating system (wipe system and load operating system)

G. RECOVERY

After the malware threat has been effectively eradicated from infected hosts the process of restoring the confidentiality, integrity, and availability of system software and data begins.

- Reinstall from backup or installation media
- Restore data from backup media
- Validate system state -The host should have security software reinstalled and the application software should be tested to ensure that it functions properly.

- Restore network connectivity

V. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

The Internal Operations Department 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.

B. NON-COMPLIANCE

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

IT13
Category: INFORMATION TECHNOLOGY

INFRASTRUCTURE FAILURE RESPONSE

I. PURPOSE

The purpose of the policy is to establish the response to any situation severely impacting business continuity. This policy will clearly define staff roles and responsibilities, to whom it applies and under what circumstances, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting and remediation mechanisms. The policy shall be well publicized and made easily available to all personnel involved in the recovery process.

II. SCOPE

This policy applies to any situation in which the Information Technology infrastructure is compromised or otherwise rendered inoperable to the extent business is unable to be conducted.

III. DEFINITIONS

"Information Technology (IT) Asset" refers to any computer hardware, network hardware, software, Information Technology-based MBCP information. In this context, "asset" and "Information Technology (IT) Asset" are understood to be the same.

"Information Technology (IT) Service" refers to any data or voice connection, file share, data store, email, communication medium. In this context, "service" and "Information Technology (IT) Service" are understood to be the same.

IV. POLICY

A. RESPONSE

When an occurrence takes place that impacts the IT infrastructure, the IT Manager will be contacted at the earliest opportunity. After the IT Manager has assessed the situation, the Director of Internal Operations will be updated along with the CEO.

The CEO will chair an incident response team to handle the incident. The team will include (based on availability) members from:

- Internal Operations;
- IT Support;
- Affected unit(s) or department(s);
- Additional individuals as deemed necessary by the CEO.

IT Support, along with the designated team, will analyze the situation to determine the effected assets and services. After the effected assets and services have been identified, IT personnel along with the Director of Internal Operations will determine the most expedient and cost-effective means of replacing the needed assets and services by reaching out to standard vendors. Every effort will be made to put in place temporary solutions to address immediate needs such as internet and phone connections along with data access requirements.

All business data is currently stored in the cloud on a secure platform. All data is accessible via secure sign-in and can be made available at any time. Should data stored on the cloud service become corrupted or otherwise made unusable, a dedicated cloud backup is in place to allow for the restoration of data.

Email is currently hosted in the cloud on a secure platform. Email is accessible via secure sign-in and can be made available at any time. Should data stored on the cloud service become corrupted or otherwise made unusable, a dedicated cloud backup is in place to allow for the restoration of data.

Servers are currently hosted in the cloud on a secure platform. The cloud hosted servers are backed up on a regular basis and restoration is available on demand.

The incident response team will communicate the decided response plan to the staff along with an estimated timeline of IT asset and service replacement and availability.

IV. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

The Internal Operations Department 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.

B. NON-COMPLIANCE

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