Food Bank For New York City IT POLICY Manual

As a not-for-profit organization we must adhere to regulations set forth by government and related contracts. Audits are conducted regularly to insure protocols are exercised within required parameters. It is the organizations responsibility to insure all computer assets including all data such as databases and file resources are secured from unauthorized use. All employees, contractors, directors, volunteers, and others authorized by management to access company resources are required to comply with these guidelines.

It is the responsibility of Food Bank for New York City authorized users to:

- Understand and comply with IT policies set forth on this document
- Use the Food Bank for New York City computer systems properly
- Protect the integrity of the systems by treating equipment with care and respecting IT security measures.
- Submit a helpdesk ticket for support when a problem occurs (**See IT Support**)

It is the responsability of the Food Bank for New York City Information Technology team to:

- Educate staff about any IT reources, questions, and/or concerns
- Follow a process that addresses IT needs in a timely manner
- Provide staff with working equipment that helps to meet their needs
- Respond to Help Desk requests in a timely manner

Management Approved Use of Computer Systems, Databases, and other IT resources

Computer systems, databases, and other IT resoucces, are to exclusively be used for conducting organization business or for purposes authorized by management. This includes but not limited to computer workstations and related peripherals, software, telephones, photocopies, Internet, and e-mails.

Use of any IT resources are subject to audit by management at any time, by way of monitoring tools in place. Provided organization resouces are not private. These resouces include but not limitted to disks and files, voice-mail, accessing the Internet, or sending e-mail. By using these IT resources, consent to monitoring is implied, with or without cause.

Software Licenses and Other Copyrighted Materials

You may not install personal or unauthorized software on our organization's computer systems. There must be a valid license for all software installed on all computer workstations. Do not copy or duplicate licensed software except if allowed by the license terms. Failure to comply may be consider theft.

Most information and software that is accessible on the internet is subject to copyright or other intellectual property right protection. Therefore, nothing should be copied or downloaded from the Internet for use within our organization unless express permission is obtained from the appropriate party. If authorized by management, a request must be submitted to the helpdesk system so software or shareware may be obtained from secure sources (**see Protecting Against Computer Viruses on this document**)

Any software or data developed at The Food Bank for New York City is the sole and exclusive property of The Food Bank for New York City.

Hardware (Including hardware issued and used offsite)

- Employees are not authorized to relocate or move any computer equipment unless authrorized by management and executed by the IT team.

- Employees are not authorized to attach/detach or install/uninstall any computer components without authorization from the IT deaprtment. This includes but not limitted to keyboard, mouse, printer, modem, monitor, internal boards, or other components. The IT department is responsible for assigning these peripherals on a needed basis.

Files, Directories and Rights

All data must be stored on designated servers, not on local hard drives (C:\, D:\, or desktop). Data on the servers are backed-up, thus protecting the user from loss of data should a computer malfunction. Data storage space on the servers is limited. If extenuating circuntances exists, request should be submitted to management to be addressed on an individual basis. If portable media containing Confidential or otherwise sensitive material, the user is responsible for storing the media in a secure locked location and delete the media when no longer needed.

- Files and/or databases are not to be assigned passwords. Any files that need to be secured should be stored within secured folders provided by the network. For assistance or clarification in this matter, please contact the Technology department.

- Access to files and/or data is determined by division director. If you believe you require access to additonal resources, communicate it to your division directors followed by a helpdesk ticket.

Purchases of IT Resources (Hardware/Software)

- All hardware\software purchases are processed by the IT Department only after proper approval from a division head.
- If additional resources outside the normal predefined setup are required, please communicate this to the appropriate division head follow by a helpdesk ticket.

System Security and Network Resources:

Employees are responsible in helping to prevent equipment theft and securing company data.

- Connecting personal laptops or equipment to the FOODBANK network is strictly prohibited.
- Use “Keyboard/Screen locks (Ctrl+Alt+Del)” to prevent unauthorized access to your workstation while away from your desk.
- When you leave your work area if health and safety regulations allow, where possible lock your office. If you use a portable computer, lock it in a desk or filing cabinet.
- Users are responsible for signing off or locking workstations at the end of each workday
- When traveling, keep portable computers in your possession at all times.

System passwords are the primary means of computer data security. You must keep your password secure and private at all times, no exceptions. Passwords must not be complex and unpredictable.

Passwords must meet the following parameters:

- Minimum of eight characters in length.
- Contain at least one alphabetic and numeric character.
- Not contain your user id or other easily identifiable sequence of characters such as child’s, spouse’s or pet’s name or birth date.
- Policy requires that password is changed every two months.
- New passwords must be unique from the last three previous passwords used.

Protecting Confidential Information

Only authorized personnel may access confidential employee data and other sensitive information. You must use security controls to manage and limit access to the information. When confidential information is stored on diskettes, CD's, memory sticks, you must keep them in a locked area when not in use. Confidential information may be printed only on a secure printer or one that you are personally watching.

You should presume that any unprotected information sent across the Internet will be read by any number of unknown people. Internet servers must never allow unrestricted access to confidential information. Confidential information accessed through or transmitted across the Internet must be protected by encryption (data or session encryption). Any of our organization's materials that are protected by copyright, which are transmitted over the Internet or by e-mail must indicate that our organization is the owner of the copyright.

Protecting Against Computer Viruses

A "computer virus" is a program designed to copy itself into other programs. The virus may also be designed to cause the loss or alteration of data on a computer, or to completely disable a computer. The virus is activated when the program "infected" is executed on a computer.

Do not load unauthorized programs onto your workstation. Be particularly alert to programs from public sources such as bulletin boards or executable files attached to e-mail messages (a sample of an excutable file is a file that its extension ends with .exe). Do not open or execute a program or file if you do not know its source.

Other forms of harmful code are not transmitted by copying and executing infected programs, but are activated by simply viewing a web site that contains maliciously programmed applets or JavaScript. Web sites established by individuals and by organizations with questionable ethics are prime candidates for hosting harmful code. You should avoid these sites at all time. Before visiting a web site for the first time, set the security control options in your web browser to prohibit execution of applets or JavaScript.

All disks, removable media, drives from any outside source MUST be scanned for viruses prior to opening the contents on the disk/removable media/drives.

We currently use TrendMicro as our antivus/spyware solution to protect our computers. This software is constanly checking your computer for any threats. If a virus infects your computer, you must inform your manager and/or contact our IT department immediately.

Internet Usage

The Internet is an important resource for our organization and should be used primarily for business transactions. Effective use of the Internet can provide improved research, better external communications and increased client responsiveness. Our Internet presence is a reflection of our image must be considered in all our Internet activities.

When accessing the Internet from a FOODBANK system you must.

- Adhere to the security and usage guidelines in this document.
- Do not place any material on the Internet that would be considered inappropriate or offensive to others and do not access such material.
- Do not access web sites that contain or distribute material that is objectionable in the workplace, including web sites that contain sexually explicit materials or advocate illegal activity.
- Streaming of music is prohibited
- Instant Messaging such as but not limited to (AOL, MSN, Yahoo and ICQ) is prohibited
- Chat Rooms / News Group: Only employees who are authorized to speak\write to the media, analysts, or public groups on behalf of The Food Bank For New York City may do so. Authorization may be granted only after the review and approval process by the appropriate division director.

Using electronic Mail

- E-Mail spoofing is prohibited (Example) Sending mail that appears to be from someone else.
- Do not send unsolicited advertising
- Do not send or reply to chain emails
- Do not reply to unsolicited non-business e-mail ("spam" or junk mail). Generally the most effective response is to delete the mailing without reading or responding

IT Support

All support questions must be submitted via the helpdesk system accessible from the employee resource page. (http://support.foodbanknyc.org/.) You can login with the same credentials that you use to login to the network. For more information on how to use the helpdesk system, please reference the employee guide provided.. Upon receipt of your helpdesk ticket, IT will respond to it within 24 Hours.

Unauthorized use of computer systems, databases, and other IT resouces could result in disciplinary action, including dismissal, criminal prosecution, and employees being held financially liable for the cost of the improper use.

I _____ have read and agree to the terms set forth in the Food Bank For New York City IT POLICY Manual.

Signature _____ **Witness**_____ **Date**_____

Employee Name Authorized Personnel