Board of Water Supply
Directive No. 501
November 1, 2019
Updated

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

1) Policy

All Board of Water Supply (BWS) Information Technology (IT) Resources are deemed BWS assets used for furthering BWS business and services. Its use is a privilege and shall be for official BWS business only.

2) Purpose

The purpose of this policy is to ensure that all users of BWS IT Resources understand and adhere to the stated acceptable uses of BWS IT Resources.

3) Scope

All users of BWS IT Resources, including employees of BWS, contractors, agents, and temporary staff, are subject to this policy.

4) Definition

a) "BWS IT Resources" include, but are not limited to, computer hardware (servers, desktops, laptops, notebooks, printers, peripherals, etc.), mobile devices (smart phones, tablets, etc.), applications/software (whether provided via or hosted/cloud based), communication services (to include wired/wireless, voice/VoIP, internal IP transport, VPN, network, and Internet or resource access), and any other IT resources provided for the express purpose of supporting BWS business requirements, which may also include City IT Resources as defined in the City and County of Honolulu Acceptable Usage of Information Technology Resources Policy.

b) "User" or "Users" means all BWS employees, contractors, consultants, temporary staff, volunteers, or others utilizing BWS IT Resources not normally available to the general public.

c) "Authorized computer hardware, or software of computer systems or networks," are defined as hardware, software, systems, and networks that were purchased, licensed, and/or installed by BWS IT or approved by BWS IT (e.g. use of City IT Resources such as the City and County of Honolulu computer network).

5) General Policy Provisions

a) Permission and Acceptance

By affixing a signature to the IT Acceptable Use policy, whether handwritten, electronic, or by other methods, the User explicitly accepts and agrees to all the terms and conditions stated in the policy. The signature must be submitted and renewed within a specified time and meet IT requirements (see IT policies, procedures, and announcements). Users with access to the online IT Acceptable Use Policy application will be required to use this system to acknowledge the compliance agreement electronically. Users without this ability will have the option to submit a handwritten signature on a printed compliance agreement

form to IT Operations. Failure to comply may result in the termination of accounts and access permissions to IT resources. To ensure safety, security, operational effectiveness, etc., IT operation policies and procedures requirements may change. User will be notified of such changes as appropriate and afforded a reasonable timeframe for compliance, given the situation. Additionally, by using any of the BWS IT Resources, the User implicitly accepts and agrees to all terms and conditions stated in this policy.

b) Privacy

Use of BWS IT Resources is primarily to conduct and support the business of the BWS. As such, Users have no proprietary interest and no reasonable expectation of privacy while using BWS IT Resources. Information stored on BWS IT Resources is not private and is the property of BWS.

Files stored on BWS IT Resources may be subject to disclosure under the U.S. Freedom of Information Act or the Hawaii Uniform Information Practices Act, criminal investigations, legal action such as a warrant or subpoena, or authorized BWS investigations. This includes backup files on BWS IT Resources and archives of electronic mail sent or received

c) Monitoring

Software may be used to identify and block access to Internet sites containing sexually explicit or other prohibited material and to monitor and filter email.

IT Resources may be monitored from time to time without prior notice to any User to ensure compliance with all IT policies, safety or security procedures, other applicable rules, regulations, and performance of BWS IT Resources.

IT Resources monitored include, but are not limited to, User access to Internet Sites, contents of emails, documents, files, blog entries, instant messaging, uploaded or downloaded data, etc.

If the monitoring is specific and due to a complaint, a reasonable suspicion of wrongdoing, or a part of a BWS-authorized investigation, the User will be informed of the monitoring in the course of the investigatory process.

Monitoring does not constitute ratification, adoption, or approval of activities occurring with BWS IT Resources

6) Responsible Use

BWS IT Resources are owned and/or controlled by the BWS and are the legal or licensed property of the BWS and are made available to Users to enable and support the activities of BWS. Users shall adhere to the "Responsible Use" guidelines which include, but are not limited to, the following:

a) Use of BWS IT Resources by Users is to be in a manner consistent with applicable BWS standards of business conduct and as part of the normal execution of an employee's job responsibilities.

b) Incidental and occasional personal use of BWS IT Resources is permitted, subject to the restrictions contained in this policy (also reference Section 7 - Prohibited Use below).

c) Communications of a sensitive or confidential nature (i.e. communications which would generally be marked CONFIDENTIAL in hard copy format) should not be sent via BWS

IT Resources unless they are encrypted. Contact the BWS IT Help Desk for assistance.

d) It shall be clear to recipients of e-mail and any other form of electronic communication (e.g. social media sites and apps, bulletin boards, chat rooms, Usenet groups, etc.) that opinions expressed by BWS users are not necessarily those of BWS.

e) Users shall keep their BWS issued Login ID and passwords safe and secured.

f) Users shall report any breaches of this policy to their supervisor. Supervisors shall then report the breach to their Program Administrator/Staff Officer, who is to report such to BWS IT.

g) Users shall store data or computer files on network shared folders or network home folders. These folders are backed up daily and can be recovered in case of computer/device failure or disaster conditions.

h) Laptops, tablets, and other BWS devices shall be connected to the BWS network during designated maintenance periods and remain connected until the required updates are complete . This is to allow the installation of software patches and upgrades to maintain the functionality of the device and to prevent vulnerability to viruses and other malicious attacks.

i) Users shall exercise reasonable care to prevent unauthorized access to BWS IT Resources and/or data (e.g. log-off computer, lock computer screen, do not share password information, etc.).

j) Users shall secure BWS IT Division approval to run non-BWS issued hardware and/or software on BWS devices, network, and/or utilizing BWS resources.

k) Users of BWS IT Resources must use ordinary care to avoid security risk, data loss, disorder, damage, or injury and shall not modify, alter, remove, or add to BWS IT Resources without explicit written authorization from BWS IT Division. Authorization shall be requested via the submittal of an IT Request form.

l) Any BWS IT Resources that are lost, stolen, or compromised must be immediately reported to BWS IT Division.

m) Users must observe all laws relating to copyright, trademark, export, and intellectual property rights.

NOTE: Since e-mail messages are perceived to be less formal than paper-based communication, there is a tendency to be lax about their content. Bear in mind that all expressions of fact, intention, and opinion via e-mail can be held against you and/or BWS in the same way as verbal and written expressions.

7) Prohibited Use

BWS explicitly prohibits all activities that are in violation of any Federal, State, or other applicable laws, rules, regulations, and established policies and procedures, except for the citations noted previously in Section 6 - Responsible Use. Prohibited uses of BWS IT Resources include, but are not limited to:

a) Gambling or illegal activities.

b) Activities that interfere with the performance of the Users or other Users' job responsibilities.

c) Promotion of BWS IT Resource use for unproductive, non-BWS related activities.

d) Access, request, display, print, use, upload, download, store (either temporarily or permanently), distribute, or send (via e-mail or any other form of electronic communication) material that is fraudulent, harassing, embarrassing, sexually explicit, pornographic, profane, obscene, indecent, racist, sexist, hateful, intimidating, abusive, defamatory or otherwise inappropriate, objectionable, offensive, or unlawful.

e) Displaying, printing, or producing sexually explicit images, text or sounds, including the foregoing where others can see or hear them.

f) Downloading or playing of games or other entertainment software (including screen savers and animations).

g) Displaying, printing, storing, or sending personal advertisements, solicitations, promotions, political, or any other unauthorized materials for non-BWS business.

h) Transmission of unsolicited bulk mail ("spamming"), transmission or forwarding electronic chain letters, or initiating or participating in the targeting of a particular person or system with mass quantities of e-mail.

i) Activities that disrupt BWS IT Resource performance, functionality, or usability.

j) Agreeing to a license, upload, download, transmission, or use of any software or cloud based (webmail, DropBox, etc.) services on or with BWS IT Resources without prior written authorization from BWS management.

k) Installing or connecting unauthorized resources,[4] including but not limited to, computer hardware,[1] software, systems, processes, etc. to BWS IT Resources, or allowing said resources to connect to questionable devices, systems, and/or networks (i.e. personal flash/thumb drives, external storage, connecting to free WIFI that has no login credentials or method of protecting user's privacy, etc.). Review and authorization by the IT Division is required before the resource can be used, installed, connected, or exposed to BWS IT resources (i.e. IT approval before consultant computer equipment can be connected to the BWS IT network).

l) Transferring[2] unauthorized computer files[3] onto BWS IT Resources.

m) Transferring[2] sensitive BWS information to and from unauthorized resources[4].

n) Sharing or publicizing confidential or proprietary information.

o) Violating copyright law and license agreement terms of copyrighted materials. A

---

[1] Memory; personal computer; monitor; scanner; printer; hard drives; CD, DVD, flash drive, memory card, tape and other removable drives; modems; video, sound, multi-media, or other expansion cards.

[2] Over the Internet, wirelessly, etc. using removable media (e.g. CD-ROM or DVD) or using any other method.

[3] Unauthorized computer files are defined as files that were not created in the process of doing BWS work. Examples include audio files, video files, graphic files, and digital photographs.

[4] Unauthorized resources are defined as any device, method, system, etc. that was not created or explicitly approved by the BWS IT Division for use in the process of doing BWS work. Examples include the use of unauthorized cloud storage or Wi-Fi connection.

violation of this policy includes unlawful file-sharing using BWS IT Resources.

p) Engaging in online chat groups, social media, streaming music or video, or other activities that create traffic loads on the network for personal non-BWS business purposes.

q) Using BWS identity (i.e. email address etc.) for online media forums, including social networking websites, mailing lists, chat rooms, and blogs, except when authorized by Manager and Chief Engineer.

r) Attempting to examine, change, or use another person's files, output, or user name, or read another user's E-mail without express permission.

s) Using another user's ID and password in order to circumvent BWS security policies.

t) Bypassing BWS virus and/or malware protection measures, to deliberately or unintentionally introduce a computer virus, worm, or other destructive/disruptive programs.

u) Bypassing BWS computer network security by accessing the Internet directly via mobile modem or other means.

v) Attempting to gain unauthorized access to BWS applications (e.g. NALU, Kronos, etc.) or information.

w) Attempting to gain access to restricted areas of the network or other hacking activities.

x) Monitoring the Internet usage of others or obtaining information through the use of IT resources without authorization.

8) Special Responsibilities of IT Staff

In addition to having all the responsibilities of any other users as described above, IT staff, including BWS employees, contractors, agents, and temporary staff, are granted certain system privileges which make it possible for them to manage the technical resources under their control. System privileges may permit access to passwords, files, voice mail, telephone, electronic communication, and other computer information and present substantial potential for abuse. Any abuse of system privileges shall be considered legitimate grounds for disciplinary action up to and including discharge and/or legal prosecution.

IT staff shall:

a) Protect individual passwords;

b) Not browse, inspect, copy, delete, rename, or modify a user's computer information without the user's permission unless required to do so as part of a duly authorized investigation or unless required to protect the security and integrity of BWS IT Resources;

c) Not collect information on individuals' computer usage unless required to do so as part of a duly authorized investigation or unless required to protect the security and integrity of BWS IT Resources;

d) Not remotely monitor or control a user's computer system without the user's permission unless required to protect the security and integrity of BWS IT

Resources. In any case, every effort shall be made to contact the user before remotely monitoring or controlling a user's computer system;

e) Keep confidential computer information viewed in the normal course of work. The use of computer information for personal or other purposes unrelated to official duties is prohibited;

f) Respect the privacy of their users' communication by configuring systems to maximize privacy;

g) Configure systems and take appropriate actions to enforce appropriate IT policies and respond to issues concerning safety and security of IT resources;

h) Provide official policies, procedures, and standards required to maintain consistency, safety, and security of BWS IT resources.

i) Remain up-to-date at all times on security issues relevant to the systems they administer;

j) Have authority to clear data, directories, files, configurations, and software from BWS devices with or without prior notice or warning, to ensure the integrity, security, and safety of BWS data, systems, operations, and customers. BWS devices that are lost or stolen will be remotely wiped to avoid compromising data contained on these devices and unauthorized use of the device(s). As a precaution, IT resource users should backup important data regularly.

k) Access, read, review, monitor, and copy all messages without the employee's consent (because e-mails, text messages, and other forms of data can be subpoenaed and are considered as evidence in judicial, civil, criminal, administrative/grievance hearings, and in disciplinary and other investigations), in order to:

   i) disclose files, text, or images to law enforcement or other appropriate third parties;
   ii) satisfy a legitimate business purpose; or
   iii) satisfy a legal obligation.

l) Provide notice to the affected employee when communications are accessed, copied, and turned over to enforcement or investigative authorities, or to third parties who presented legal subpoenas and authorization for such information.

i) Act promptly to address abuses upon notification.

9) Non-Compliance

All users have a responsibility to use BWS IT Resources in a professional, lawful, and ethical manner. Non-compliance with the BWS policy on acceptable use of Information Technology resources may result in revocation of privileges and/or disciplinary action, up to and including discharge from employment and, if warranted, civil penalties or criminal prosecution.

REVIEWED AND APPROVED:

9/1/2020

ERNEST Y.W. LAU, P.E. Date
MANAGER AND CHIEF ENGINEER