Subject: Acceptable Use Policy

Policy No: 2015-62
Effective Date: 07.01.21

1) Overview:

The intent for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to the Benton-Franklin Workforce Development Council's (BFWDC) established culture of openness, trust, and integrity. We are committed to protecting BFWDC's employees, board members, workforce partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfer protocol (FTP), are the property of BFWDC. These systems are to be used for business purposes in serving the interests of the company, and our clients and customers during normal operations.

Remote access to our corporate network is essential to maintain our team's productivity, but in many cases, this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of the BFWDC, we must mitigate these external risks to the best of our ability.

E-mail is widely used in almost all industries and is often the primary communication and awareness method within an organization. At the same time, misuse of e-mail can pose many legal, privacy, and security risks, thus it's important for users to understand the appropriate use of electronic communications.

Effective security is a team effort involving the participation and support of every BFWDC employee who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2) Purpose:

The purpose of this policy is to outline the acceptable use of the network, remote access, e-mail, and computer equipment at BFWDC. These rules are in place to protect the employee and BFWDC. Inappropriate use exposes BFWDC to risks, including virus attacks, compromise of network systems and services, loss of sensitive or confidential data, and legal issues.

3) Scope:

This policy applies to the use of information, electronic and computing devices, and network resources to conduct BFWDC business or interact with internal networks and business systems, whether owned or leased by BFWDC, the employee, or a third party. All employees, contractors, and consultants at BFWDC are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with BFWDC policies, standards, and local laws and regulations.

This policy applies to employees, contractors, and consultants at BFWDC, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by BFWDC.

4) Policy:

4.1. General Use and Ownership

4.1.1. BFWDC proprietary information stored on electronic and computing devices, whether owned or leased by BFWDC, the employee or a third party, remains the sole property of BFWDC.

4.1.2. You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of BFWDC proprietary information.

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

4.1.4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

4.1.5. For security and network maintenance purposes, authorized individuals within the BFWDC Information Technology (IT) Contractor may monitor equipment, systems, and network traffic at any time.

4.1.6. BFWDC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2. Security and Proprietary Information

4.2.1. Postings by employees from a BFWDC e-mail address to newsgroups (local news stations, social media, newspapers, radio, bloggers, etc.) must first be approved by the Chief Executive Officer (CEO) or the Chief Operations Officer (COO) and may be required to include a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of BFWDC, unless posting is in the course of business duties.

4.2.2. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.2.3. Automatically forwarding e-mail – employees must exercise caution when sending any e-mail from inside BFWDC to an outside network. Unless approved by the CEO or COO, BFWDC e-mail will not be automatically forwarded to an external destination. Copying e-mail outside of the BFWDC network for purposes of storage is prohibited.

4.2.4. Security Software Guidelines – recommended process to prevent virus problems:

- **a)** NEVER click on any links, or open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- **b)** Delete spam, chain, and other junk e-mail without forwarding.
- **c)** Never download files from unknown or suspicious sources.
- **d)** Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- **e)** Any attempts to disable to circumvent security software, policies, or restrictions are strictly prohibited.

4.3. E-mail Policy

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

4.3.2. BFWDC e-mail account should be used primarily for BFWDC business-related purposes; personal communication is permitted on a limited basis, but non-BFWDC related commercial uses are prohibited (i.e., do not use BFWDC e-mail to sign up for eBay or Amazon).

4.3.3. E-mail should be retained if it qualifies as a BFWDC business record. E-mail is a BFWDC business record if there exists a legitimate and ongoing business reason to preserve the information contained in the e-mail.

4.3.4. E-mail that is identified as a BFWDC business record shall be retained according to BFWDC Record Retention Schedule. All BFWDC e-mail information is categorized into three main classifications with retention guidelines:

a) Administrative Correspondence (3 years)

b) Fiscal Correspondence (3 years)

c) General Correspondence (1 year)

4.3.5. Using a reasonable amount of BFWDC resources for personal e-mails is acceptable, but non-work-related e-mail shall be saved in a separate folder from work-related e-mail. Sending chain letters or joke e-mails from a BFWDC e-mail account is prohibited.

4.3.6. BFWDC may monitor messages without prior notice. BFWDC is not obliged to monitor e-mail messages.

4.4. Remote Access

It is the responsibility of BFWDC employees, contractors, vendors, and agents with remote access privileges to BFWDC's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to BFWDC.

When accessing the BFWDC network from a personal computer, Authorized Users are responsible for preventing access to any BFWDC computer resources or data by non-Authorized Users. Performance of illegal activities through the BFWDC network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. Authorized Users will not use BFWDC networks to access the Internet for outside business interests (i.e., using the shared drive for personal purposes).

4.4.1. Secure remote access to the BFWDC Virtual Private Network (VPN) will be monitored and regulated by the Information Technology (IT) Contractor.

4.4.2. Authorized Users shall protect their login and password, even from family members.

4.4.3. While using a BFWDC-owned computer to remotely connect to BFWDC's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.4.4. Use of external resources to conduct BFWDC business must be approved in advance by the CEO or COO.

4.5. Internet Use Monitoring and Filtering

4.5.1. Web Site Monitoring: BFWDC reserves the right to monitor and filter internet and website traffic. The IT Contractor may monitor Internet use from all computers and devices connected to the corporate network. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

4.5.2. Internet Use Filtering System: The IT Contractor may block access to Internet websites and protocols that are deemed inappropriate for BFWDC's corporate environment. BFWDC staff are prohibited from visiting the following protocols and categories of websites:

- **a)** Adult/Sexually Explicit Material
- **b)** Advertisements & Pop-Ups
- **c)** Gambling
- **d)** Hacking
- **e)** Illegal Drugs
- **f)** Personals and Dating
- **g)** SPAM, Phishing and Fraud
- **h)** Spyware
- **i)** Violence, Intolerance, and Hate

4.5.3. Internet Use Filtering Rule Changes: The IT Contractor may periodically review and recommend changes to web and protocol filtering rules. The CEO or COO shall review these recommendations and decide if any changes are to be made.

4.5.4. Internet Use Filtering Exceptions: If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the IT Contractor help desk. An IT employee will review the request and un-block the site if it is miscategorized.

4.5.5. Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must get approval from the CEO or COO, who will coordinate with the IT Contractor.

4.6. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempt from these restrictions during their legitimate job responsibilities.

Under no circumstances is an employee of BFWDC authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing BFWDC-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.6.1. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

a) 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 BFWDC.

b) 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 BFWDC or the end-user does not have an active license is strictly prohibited.

c) Accessing data, a server, or an account for any purpose other than conducting BFWDC business, even if you have authorized access, is prohibited.

d) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

e) Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

f) Using a BFWDC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

g) Making fraudulent offers of products, items, or services originating from any BFWDC account.

h) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

i) 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.

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

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

l) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

m) Providing information about, or lists of, BFWDC employees to parties outside BFWDC.

n) Moving data outside of the BFWDC network for storage purposes is prohibited.

4.6.3. E-mail and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Questions may be addressed to the COO.

a) Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).

b) Any form of harassment via e-mail, telephone, or paging, whether through language, frequency, or size of messages.

c) Unauthorized use, or forging, of e-mail header information.

d) Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

e) Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

f) Use of unsolicited e-mail originating from within BFWDC's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by BFWDC or connected via BFWDC's network.

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

h) Users are prohibited from automatically forwarding BFWDC e-mail to a third-party e-mail system

4.6.4. Blogging and Social Media

a) Blogging by employees, whether using BFWDC's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of BFWDC's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate BFWDC's policy, is not detrimental to BFWDC's best interests, and does not interfere with an employee's regular work duties. Blogging from BFWDC's systems is also subject to monitoring.

b) Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of BFWDC and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging.

c) Employees may also not attribute personal statements, opinions, or beliefs to BFWDC when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of BFWDC. Employees assume all risks associated with blogging.

5) Compliance:

5.1. Verification, Exceptions, Non-Compliance

5.1.1. Compliance Measurement

The CEO or COO will verify compliance to this policy through various methods, which may include, but are not limited to, internal and external audits.

5.1.2. Exceptions

Any exception to the policy must be approved by the CEO or COO as their proxy.

5.1.3. Non-Compliance

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