ICT CODE OF CONDUCT

Date of adoption: 23 May 2017
Council resolves to adopt the under-mentioned revised policy as the Information Technology Policy of the DR BEYERS NAUDE LOCAL Municipality.

Table of contents

1. OVERVIEW

Beyers Naudé Local Municipality's (BNLM) intention for publishing an ICT Code of Conduct is not to impose restrictions that are contrary to its established culture of openness, trust and integrity. BNLM is committed to protecting its employees, 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, WWW browsing, and FTP, are the property of BNLM. These systems are to be used for business purposes in serving the interests of the municipality in the course of normal operations.

Effective security is a team effort involving the participation and support of every BNLM employee and affiliate 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.

This administrative Code of Conduct statement sets forth the Code of Conduct of BNLM with regard to use of, access to, and disclosure of electronic mail and network resources to assist in ensuring that the municipal resources serve those purposes.

2. SYSTEM AND NETWORK ACTIVITIES

The following activities are strictly prohibited, with no exceptions:

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, installation or distribution of "pirated" or other software products that are not appropriately licensed for use by BNLM.

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

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

Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

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

Revealing your account and Wi-Fi password to co-workers or none BNLM employees or allowing use of your account by co-workers. This includes family and other household members when work is being done at home.

Using a BNLM 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.

Making fraudulent offers of products, items, or services originating from any BNLM account.

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

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 authorised 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.

Port scanning or security scanning is expressly prohibited unless prior notification to BNLM is made.

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.

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

Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

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.

The deliberate transmission of computer viruses, worms, Trojan software, or other malicious programs.

Interfering with, disrupting, or denying service including, but not limited to, using any technique to intentionally degrade or disable the delivery of any legitimate data (e.g., denial of service attacks).

Attempting to gain unauthorized entry to any site or network including but not limited to executing any form of network probing, monitoring or other information-gathering on someone else's site or network.

Attempting to circumvent host or user authentication or other security measures of any host, network or account.

Attaching devices to the physical infrastructure of the network without prior authorization from the ICT Unit.

Installation of Software without the express permission of the ICT Unit.

Interference with systems including, but not limited to, removal or change of internal parts.

Providing information about, or lists of, BNLM employees to parties outside BNLM

3. EMAIL AND COMMUNICATIONS ACTIVITIES

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Violates or infringes on the rights of any other person, including the right to privacy.
4. Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or illegal.
5. Messages that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, or religious or political beliefs.
6. Violates municipal or departmental regulations prohibiting sexual harassment.
7. Restricts or inhibits other users from using the system or the efficiency of the computer systems.
8. Encourages the use of controlled substances or uses the system for the purpose of criminal intent.
9. Uses the system for any other illegal purpose.
10. Conduct any non-approved business.
11. Solicit the performance of any activity that is prohibited by law.
12. Transmit material, information, or software in violation of any municipal law.
13. Conduct any non-governmental-related fund raising or public relations activities.
14. Engage in any activity for personal gain.
15. Make any unauthorized purchases
16. Unauthorised use, or forging, of email header information.

17. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

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

19. Use of unsolicited email originating from within BNLM networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by BNLM or connected via BNLM networks.

20. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

21. Sending unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, who were not previous customers or with whom the sender did not have an existing business relationship ("E-mail spam"). BNLM reserves the right to determine in its sole discretion and based on the information available (1) what constitutes spam as well as (2) what measures are necessary in response to spamming complaints.

22. Harassment including, but not limited to, through language, frequency or size of messages.

23. Unauthorized use, or forging, of mail header information.

24. Solicitations of mail for any other E-mail address other than of the poster's account or service with the intent to harass or to collect replies.

25. Creating or forwarding "chain letters" or other “schemes" of any type.

26. BNLM also reserves the right to monitor any content that passes through the mail system as well as enforcing content filtering mechanisms that are deemed necessary.

27. Because electronic messages are typically stored in one place and then forwarded to one or more locations, often without the specific knowledge of the originator, they are vulnerable to interception or unintended use. The Municipality will attempt to provide an electronic messaging environment, which provides data confidentiality and integrity. The Municipality cannot be responsible for web-based e-mail systems, however, such as Yahoo, Juno, etc. Municipal employees should always be aware of the risks.

28. Use of unsolicited E-mail originating from within BNLM network or networks of other Internet Service Providers on behalf of, or to advertise any service hosted by BNLM, or connected via BNLM network.

4. BLOGGING (put definition)

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

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

3. Employees may also not attribute personal statements, opinions or beliefs to BNLM 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 BNLM (previously Cacadu District Municipality). Employees assume any and all risk associated with blogging.

4. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, BNLM trademarks, logos and any other BNLM intellectual property may also not be used in connection with any blogging activity

5. INTERNET

All private use of Municipalities Internet / E-mail systems must occur outside normal working hours and may not be to the prejudice of the Municipality.

The same standards of conduct apply to employees for personal use as that set out for business use. Employees should note that they are directly and personally liable and responsible for any obligations, illegal activities, commitments, undertakings, or any other abuses that may occur.

All employees who use the Internet / E-mail for personal use shall indemnify and hold the Municipality harmless against all claims, losses and costs the Municipality may become liable for by reason of such use and hereby authorize the Municipality to make deductions from and to retain from wages any amount necessary to entirely discharge this liability.

Internet access provides necessary access to information for many municipal employees. Employees are responsible for making sure they use this access correctly and wisely.

Inappropriate uses of the Internet include, but are not limited to:

1. Viewing, downloading or sending pornographic materials.
2. Visiting and/or participating in chatrooms not designed for professional interactions specifically related to one's job.
3. "Surfing" the Web for inordinate amounts of time.
4. Otherwise endangering productivity or the Municipality.

Such matters will be construed as gross misconduct.

6. GENERAL RULES

6.1 INTERNET USER INDEMNITY

1. Only I shall have access to my Internet name and password and will not hand it out to anyone except my supervisor. Should I give my password to anyone else, I will still be held responsible for my Internet account.
2. I will log out of Internet, if the workstation is unattended for a period of time.
3. I will not abuse my Internet account by accessing sites which are deemed obscene or defamatory.

4. I will not download material that has no relation to my job function.

5. I will not download anything of a pornographic nature.

6. I will not download or install any illegal software

7. I will only use my Internet for company sanctioned business reasons. Limited personal use of the Internet is permitted'. However if this facility is abused, or is contrary to any of the other rules it will be revoked!

8. I understand that my Internet usage will be monitored as part of normal systems administration.

It should be understood that if the above is not adhered to, disciplinary action can be taken, up to and including dismissal.

I have read and understood the **Internet user indemnity**.

Initial:	

6.2 NETWORK USER INDEMNITY FORM

General Username and Password Rules:

I undertake to guard the confidentiality of the information to which I will be granted access, by adhering to the following rules:

1. Only I shall have access to my Username and Password and will not divulge it to anyone nor shall I write down my Password and leave it where the security thereof may be compromised.

2. Should I divulge or inadvertently compromise the security of my Username and Password, I understand that I will be held responsible for all transactions performed on my workstation with my allocated Username.

3. I shall ensure that my workstation is logged out of the network system or locked when unattended for a period of time.

4. I shall change my Password as and when prompted to do so by the system.

5. I shall conform to the standards set in the Strong Password Security Code of Conduct attached hereto.

6. I shall, at all times, take good care of my workstation as it is a valuable company asset and report any problem(s) to the ICT Department immediately.

7. I undertake not to download or install, any unauthorized applications, unless cleared with the Systems Administrator.

8. I will not make copies of any software and/or data and remove it from the premises without prior arrangement with the Systems Administrator.

9. If I store (data) information on my hard drive, I am responsible for backups of the data or I will make arrangements with the ICT Unit to do so periodically.

10. I understand that the content of my network drives will be monitored as part of normal system administration.

11. I understand that the remote control feature may be used from time to time in the process of end user support, computer asset control and network problem solving.

It should be understood that if the above is not adhered to, disciplinary action can be taken, up to and including dismissal.

I have read and understood the **Network user indemnity**.

Initial:	

6.3. PASSWORD SECURITY CODE OF CONDUCT

What is Password Strength? Password Strength is a measure of the effectiveness of a Password in resisting guessing and brute-force attacks. The strength of a Password is a function of length, complexity, and unpredictability. Strong Passwords meet a number of requirements for complexity - including length and character categories - that make Passwords more difficult for attackers to determine. Establishing Strong Password policies for your organization can help prevent attackers from impersonating users and can thereby he prevent the loss, exposure, or corruption of sensitive information.

BNLM's Password Code of Conduct is defined by means of the following Microsoft Active Directory attributes:

- **Enforce Password History:** The BNLM Password Code of Conduct states that no user will be able to use the same Password until a 12 month period has elapsed.
- **Maximum Password Age:** The BNLM Password Code of Conduct states that your Password will be set to expire every 30 days. You will be prompted by the system before this 30 day time elapses notifying you that you have x number of days left before your Password expires.
- **Minimum Password Age:** The BNLM Password Code of Conduct states that you will be required to use your new Password you have just changed to before you are able to manually change it yourself again.
- **Minimum Password Length:** The BNLM Password Code of Conduct states that you will be required to have a Password of no less than 6 characters.
- **Passwords must meet the specified complexity requirements:** The BNLM Password Code of Conduct states that the Password structure should meet the following requirements:

  The Password must contain at least one character from each of the following four character sets:

- English uppercase characters (A - Z)
- English lowercase characters (a * z)
- Base 10 digits (0 - 9)
- Special characters (!, $, #, %)

  It should be understood that if the above is not adhered to, disciplinary action can be taken, up to and including dismissal.

I have read and understood the **Password Security Code of Conduct.**

Initial:	

7. REGULATION AND ENFORCEMENT

Municipal Directors (or their delegated representatives) are responsible for compliance with provisions of this Code of Conduct and for investigating suspected non-compliance. These duties include, but are not limited to:

1. Investigation of alleged or suspected non-compliance with the provisions of the Code of Conduct; and

2. Suspension of service to users or of user access with or without notice when deemed necessary for the operation and/or integrity of the Municipalities communications infrastructure or connected networks.

3. When an instance of non-compliance is suspected or discovered in a computing system or network the Municipality shall proceed in accordance with Municipalities disciplinary process detailed in the collective agreement. Internal discipline, up to and including termination of services, may be appropriate in some cases of non-compliance with this Code of Conduct. Criminal or civil action may be initiated in appropriate instances.

7 DECLARATION

I have read and fully understand the content of this Code of Conduct and I agree to operate within the boundaries of this Code of Conduct.

Employee Name:_____ Date: _____

Employee_____ Signature: _____