ADMINISTRATIVE POLICY NO. 14-04

INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICY

I. INTRODUCTION

Information and communication technologies (ICT), consisting of computers and telecommunications and network resources, are provided by the CBJ to aid its employees in accomplishing the CBJ's objectives. The purpose of this policy is to establish a uniform guideline for the use of ICT. All users when connected to the CBJ networks from private devices as well as CBJ devices are subject to this policy.

CBJ users, including employees, contractors, and volunteers, who violate this policy are subject to discipline up to and including termination from service.

II. ICT POLICY

A. All information transmitted received or stored on CBJ ICT is subject to review by, or at the direction of CBJ management. Users should not have any expectation of privacy in the use of the CBJ ICT. The CBJ reserves the right to monitor and review any communications, files, or other use of CBJ ICT without any advance notice to, or the consent, of any user.

B. All files and email messages saved on CBJ ICT may be considered a matter of public record and subject to disclosure. This includes all files, email messages, or text transmitted, received, or saved on any personal computing equipment (phones, smartphones, tablets, computers, etc.).

C. Incidental personal use, in compliance with the other provisions of this policy, is allowed as long as it does not:
   1. Interfere with the business of the CBJ, or any employee's job performance.
   2. Consume significant resources.
   3. Give rise to additional costs.
   4. Create personal financial gain unrelated to a user's duties with the CBJ, unless the ICT being accessed and used is a bulletin board or web page made available by the CBJ MIS Division for the purpose of enabling employees to market and sell personal property.

D. CBJ users shall take reasonable precautions to protect access codes, computer passwords or other access mechanisms to avoid unauthorized access. Passwords for systems are created by users for the purpose of excluding unauthorized personnel, not to provide privacy from official review. CBJ users must not divulge their passwords to any other person. Password criteria and other computer policies established by MIS can be found on the MIS intranet page.

E. Only encryption tools authorized by MIS may be used. Except with the prior written consent of the MIS director, all such tools must be implement key-recovery or key-escrow techniques to permit the CBJ to access and recover all encrypted information (e.g., in the case of the absence of the employee who performed the encryption).

F. Confidential information (whether owned by the CBJ, its vendors, or other persons) is not to be disclosed to others without prior authorization. The question of "authorization" will be a function of the type and ownership of the confidential information. (For example, different authority may be required for disclosure of CBJ-owned information than for vendor-owned information). "Authorization" for disclosure may be limited to certain specific individuals within the agency on a need-to-know basis.

G. Users are expressly prohibited from engaging in the following acts. Doing so may subject a user to removal of use privileges and/or disciplinary action, up to and including termination of employment:

   1. Engaging in any willful act or omission that may cause a general loss of computer, telecommunications equipment, or network resources, or that will interfere with any CBJ functions.
   2. Using any CBJ ICT for illegal activity.

3. CBJ users shall access, delete, examine, copy, modify, and retrieve any stored information only to accomplish the CBJ's objectives.
4. ICT shall not be used for financial or personal gain such as running any aspect of a private business, or for the purpose of advocating voting for or against a candidate for federal, state, or municipal office, or a federal, state, or municipal ballot issue, not directly related to the user's work duties. Use of the CBJ's intranet bulletin board to advertise sale items, make global announcements, etc., is exempt from this restriction.
5. The installation or use of any software or hardware on CBJ ICT without prior approval from the user's department director or MIS is prohibited.
6. CBJ users may not download, install, duplicate, or store software or data files that violate applicable copyright or license agreements.
7. CBJ users shall not attempt to circumvent or subvert the CBJ ICT systems or processes intended to protect and secure CBJ information.
8. CBJ users may not use CBJ ICT to store, print, distribute, edit, record or display offensive, defamatory, discriminatory, harassing, disruptive or any other prohibited material, unless explicitly authorized to do so to accomplish the CBJ's objectives.
9. CBJ users may not attempt to gain unauthorized access or attempted access to any other person's computer, email, or voicemail accounts or equipment.
10. Under no circumstances may any posting, message, or document originating at the CBJ be in violation of the letter or the spirit of the CBJ's policies, such as the Equal Employment Opportunity or Harassment policies.
11. CBJ users shall not misrepresent their identity in any way while using CBJ ICT. This includes using another employee's email account, or by modifying another's messages without permission. The content of messages written by others should be forwarded with no changes, except to the extent that edits to the original message are clearly indicated (for example, by using brackets or by using other characters such as * * * to flag edited text).
12. Connecting directly to the CBJ computing or networking systems with a personal device without direct authorization from MIS is prohibited. Remote access rules and criteria for using personal devices to connect the CBJ computing and network resources are driven by MIS. Users are required to comply with any rules posted by MIS on the MIS home page under the link called Computer Policies.

H. All users shall take immediate action to address any inadvertent violation of these rules by immediately contacting MIS, providing specific information describing the violation.

III. RETENTION AND SECURITY OF E-MAIL MESSAGES

Email messages and computer-stored items are CBJ property and are public documents. Email messages are official documents until they are destroyed, and may have legal and operational effect identical to that of traditional, hardcopy documents. Accordingly, all email messages should be treated as though they may later be viewed by others.

They must be administered as required by the Alaska Archives Act, the Alaska Open Records Act, and CBJ document retention policies. In addition, messages may become evidence in a lawsuit and thus subject to the rules of court regarding discovery. *Do not attempt to evade these requirements by moving or destroying documents in response to legitimate requests under the Open Records Act or because a lawsuit has been or probably will be filed.* Any such attempt is illegal, is detectable, and will subject the CBJ and you to severe penalties.

It is the policy of the CBJ that email messages are temporary informal documents that are routinely destroyed after 90 days unless users make a deliberate decision to preserve them. Users are required to administer email messages generated and received via CBJ ICT as follows:

A. Immediately upon sending or receiving a message, users should make a determination whether the message has any lasting administrative, legal, or historical value, or if it is evidence in a pending or probable lawsuit.

B. If the message has no lasting value and does not constitute evidence, users may delete it or may leave it in the Inbox. The Inbox, Deleted Items, and Sent Items folders are set to automatically purge all messages older than 90 days.

C. If the message has any lasting administrative, legal, or historical value, or if it is evidence in a pending or probable lawsuit, the message should be moved from the Inbox or Sent Items folders folder and preserved in an Outlook folder that is not automatically purged.

IV. GENERAL PROVISIONS

Scope: This policy applies to all agencies and employees of the City and Borough of Juneau, Alaska.

A. Authority to promulgate policy: The City Manager of the City and Borough of Juneau, Alaska, maintains the authority granted by the CBJ Charter to order policy and the guidelines for implementation.

B. Effective Date: This policy will take effect on date policy is signed.

Dated at Juneau, Alaska, this 9th day of December, 2014.

Kimberly A. Kiefer
City and Borough Manager