BOISE COUNTY

RESOLUTION #2019-13
A BOISE COUNTY RESOLUTION ADOPTING THE BOISE COUNTY PASSWORD POLICY

WHEREAS, the Board of Boise County Commissioners has reviewed the Boise County Password Policy; and

WHEREAS, a diligent review and discussion of the policy, has been accomplished by the Board of Boise County Commissioners, with the help of the IT Support Technician; and

WHEREAS, an agreement has been reached by the Board of Boise County Commissioners and the IT Support Technician on the Password Policy; and

WHEREAS, the Board of County Commissioners recognizes the need for amendments to the procedures utilized within the password policy; and

NOW THEREFORE BE IT RESOLVED, that the Board of Boise County Commissioners does hereby rescind Boise County Resolution #2017-04; and

IT IS FURTHER RESOLVED that Resolution #2019-13, known as the Boise County Password Policy, be effective as of January 29th, 2019.

APPROVED and ADOPTED this 29th day of January, 2019, in Open Session of the Boise County Board of County Commissioners.

BOISE COUNTY BOARD OF COMMISSIONERS

ALAN D. WARD, Chairman

ABSENT

ROGER B. JACKSON, Commissioner

LAURA L. BAKER, Commissioner

ATTEST:

Mary Prisco

Mary T. Prisco, Clerk to the Board

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of Boise County's entire network. As such, all Boise County employees (including contractors and vendors with access to Boise County systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

2.0 Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, the accounts of those passwords, and the frequency of change. Guidelines from the US federal government via NIST will be used.

3.0 Policy

3.1 General

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 365 days and cannot be reused.
- User accounts with access to ILETS/NCIC privileges must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level, system-level, email, and ILETS/NCIC access level passwords must conform to the guidelines described below.

3.2 Guidelines

Password Construction Requirements

i. Be a minimum length of 12 (12) characters, recommend one upper case, one lower case, one number or symbol.
ii. Not be the same as the User ID.
iii. Expire within a maximum of 365 calendar days.
iv. Not be identical to the previous passwords.
v. Not be transmitted in the clear or plaintext outside the secure location (via text message, instant message etc).
vi. Not be displayed when entered.
vii. Ensure passwords are only reset for authorized user.

3.3 Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

- When a user retires, quits, is reassigned, released, dismissed, etc.
- Default passwords shall be changed immediately on all equipment.

When a password is no longer needed, the following procedures should be followed:

- Employee should notify his or her immediate supervisor.
- Supervisor or POC should fill out a password deletion form and send it to CAI.
- CAI POC will then delete the user's password and delete or suspend the user's account.
- The supervisor will then check to make sure the account and password have been suspended and deleted and filed in the employee's personnel file the employee was terminated / resigned / retired.

3.4 Password Protection Standards

- Do not use your User ID as your password.
- Do not share [agency name] passwords with anyone, including administrative assistants or secretaries.
- All passwords are to be treated as sensitive, Confidential Boise County information.

Here is a list of "do not's"

- Don't reveal a password over the phone to anyone.
- Don't give your password to anyone, even IT.
- Don't reveal a password in an email message.
- Don't reveal a password to the boss.
- Don' talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to a co-worker while on vacation.
- Don't use the "Remember Password" feature of applications.
- Don't write passwords down and store them anywhere in your office.
- Do not use your Boise County passwords on any external web sites or programs unrelated to Boise County.
- Don't store passwords in a file on ANY computer system unencrypted. If someone demands a password, refer them to this document or have them call your agency head or CAI POC.

If an account or password is suspected to have been compromised, report the incident to CAI POC and change all passwords. Password cracking or guessing may be performed on a periodic or random basis by the CAI POC. If a password is guessed or cracked during one of these scans, the user will be required to change it.

3.5 Remote Access Users Access

Remote User Access to the Boise County networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required) or a

form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.) or other CAI approved method (i.e, rd_app).

4.0 USB Devices

USB Usage

Using USB devices from any external or uncontrolled environment is a security concern. They can contain malware and spread infection as soon as they are connected to a network.

The only way to completely protect the system from USB based risks is to not allow them to be plugged in at all. Each county employee will carefully evaluate the necessity of USB use. If the use of USB devices is critical to your organization and banning them is not an option, here are the measures that will be taken to secure data:

i. Only use county approved USB devices (to be reviewed and approved by CAI).
ii. Under no circumstances should a personal USB device be plugged into a Boise County system. (for a complete list of USB security information, see CAI's USB Usage Recommendations)

5.0 Penalties

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

ACKNOWLEDGMENT OF RECEIPT OF PASSWORD POLICY

I, _____ acknowledge receipt of the Boise County Password Policy, effective as of January 29th, 2019.

Please initial each statement below if it is true.

____ I understand that it is my responsibility to read and understand the contents of this Policy.

____ I understand that I am obligated to perform my duties of employment in conformance with the provisions of this Policy and any additional rules, regulations, policies or procedures imposed by the department in which I work whether or not I choose to read the Policy.

____ I understand that this Policy may be modified without prior notice to me.

____ I understand that should this Policy be modified that I will be provided with a copy of the modification.

DATED this _____ day of _____, 20___.

_____
(*Employee)*

I, _____, provided a copy (either electronically or by paper) of the Password Policy, as adopted by the governing Board on _____ to _____, on this _____day of _____, 20__.

_____
(Name - Title - Department)