BOISE COUNTY

RESOLUTION #2017-04
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 a policy, has been accomplished by the Board of Boise County Commissioners, with Elected Officials and Department Heads; and

WHEREAS, agreement has been reached by the Board of Boise County Commissioners, Elected Officials and Department Heads on the Password Policy.

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

IT IS FURTHER RESOLVED that Resolution #2017-04, known as the Boise County Password Policy, be effective as of November 15th, 2016.

APPROVED and ADOPTED this 15th day of November, 2016, in Open Session of the Boise County Board of County Commissioners.

BOISE COUNTY BOARD OF COMMISSIONERS

ALAN D. WARD, Chairman

ROGER B. JACKSON, Commissioner

LAURA L. BAKER, Commissioner

ATTEST:

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.

3.0 Policy

3.1 General

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot reuse any of the past 10 passwords.
- 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 eight (8) characters on all systems, with password including at least one upper case letter, one lower case letter, and then at least either one symbol or one number.
ii. Not be the same as the User ID.
iii. Expire within a maximum of 90 calendar days.
iv. Not be identical to the previous ten (10) 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.