DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

Internal Operations Manual

SUBJECT: Password Policy	**NUMBER:**	107-01-140
DIVISION: Operations	**EFFECTIVE DATE:**	4-4-07

APPROVED: Lindsay A. Ball

POLICY/ PURPOSE: To ensure that access to sensitive data is appropriately safeguarded, all authorized users with access to the Department of Administrative Services network via active directory login on a desktop, laptop, mobile device, or remote access are responsible for selecting and securing passwords. Passwords are to be used with unique user names and are to be updated regularly.

AUTHORITY: ORS 291.037 and ORS 291.038; DAS Acceptable Use Policy

APPLICABILITY: All DAS employees; applicable to laptops and desktop computers.

ATTACHMENTS: None

DEFINITIONS: None

GUIDELINES: Passwords must be a minimum of eight characters and must be changed every 90 days. A new password is required every 90 days, as password cannot be recycled.

Passwords must include at least one numeric character and may include special characters such as $, @, #, etc. Inclusion of a special character is highly recommended. Passwords may not include personal information such as date of birth, dog's names, etc.

To increase security, passwords should not use words and should not contain consecutive or repeating characters such as "zzzzzzz" or "12345".

Passwords must not be shared with others, including supervisors, IT staff, and administrative assistants. People needing access to a computer, application, or file or file structure should contact the Technology Support Center for assistance. Passwords must be changed immediately if compromised or suspected to be compromised. All new employees are required to change their password from the Welcome Password at first login.

Automated logins are not allowed.