USER ACCOUNT POLICY

INTRODUCTION

Computer accounts are the means used to grant access to Alabama Department of Postsecondary Education (DPE) Information Resources. These accounts provide a means of providing accountability, a key to any computer security program, and access to information and documents. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

1.0 – POLICY

1.1 All accounts created must have an associated request and approval that is appropriate for the DPE system or service.

1.2 All users must sign the **Statement of Understanding Computer Systems Acceptable Use Policy** before access is given to an account.

1.3 All accounts must be uniquely identifiable using the assigned user name.

1.4 All default passwords for accounts must be constructed in accordance with the **DPE Password Policy**.

1.5 All accounts must have a password expiration that complies with the **DPE Password Policy**.

1.6 Accounts of individuals on extended leave (more than 30 days) will be disabled.

1.7 All user accounts that have not been accessed within 30 days will be disabled.

1.8 User accounts of separated personnel shall, be immediately by disabled, removed from all security groups, have all Exchange permissions revoked, and have the password changed in a manner that is in accordance with the **DPE Password Policy**. After the email archive process outlined in the **DPE Email Access Policy** is complete, the user account shall be deleted.

1.9 System Administrators or other designated staff:

- are responsible for removing the accounts of individuals that change roles within DPE or are separated from their relationship with DPE
- must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
- must have a documented process for periodically reviewing existing accounts for validity
- are subject to independent audit review
- must provide a list of accounts for the systems they administer when requested by authorized DPE management
- must cooperate with authorized DPE management investigating security incidents

2.0 – PROCEDURES

2.1 A request for a new account may be sent the IT Division through a variety of methods, phone call, email, or a help desk ticket. In all cases, the request is to be entered into the help desk system for documentation.

2.1.1 Any requests for a user account for part-time employees, consultants, vendors and/or agents shall require the Director of Information Systems to submit for approval by the Vice Chancellor of Finance and Administrative Services and the Deputy Chancellor.

2.2 On consultation with the Director of Information Systems, an account manager of the IT Division shall determine in which security groups an account needs to be placed.

2.3 There are three types of User/Network accounts used by DPE:

2.3.1 **Individual Accounts** are the primary and preferred method of providing access to resources. Users are accountable to their actions and can be audited by the systems to which they have access rights.

2.3.2 **Administration (Privileged) Accounts** can be granted to IT Administrative/Operational staff that permit elevated access rights to specific systems or applications support and maintenance. Generic/built-in privileged accounts (e.g., Windows domain and local administrator, etc.) shall not be used for daily systems administration. Use a company privileged account instead

2.3.2.1 There shall only be two members of the IT Staff within the Enterprise Admins group, the Director of Information Services and the Network Administrator.

2.3.2.2 Other IT Staff shall be placed into specialized administration groups that allow them to only perform certain management tasks.

2.3.2.2.1 Server Operators Group – IT Staff who require access and elevated privileges to manage and maintain servers may be placed in this group

2.3.2.2.2 Account Operators Group – IT Staff who require access and elevated privileges to manage and maintain user accounts and groups may be placed in this group.

2.3.2.2.3 Back up Operators Group – IT Staff who require access and elevated privileges to perform backup and restore operations on servers may be placed in this group.

2.3.2.2.4 No IT staff shall be placed in more than two of the specialized administration groups.

2.3.3 **Application-Specific Accounts** can be granted to an application available on the network that needs access to network resources. Access rights and privileges are

programmed/configured within the application. These accounts must never be used for individual access to the network itself.