Information Technology Group
Policy Name: Directory Services Account Management Policy
Date Issued: 12/15/2012
Date Last Updated: 02/06/2018

1. Introduction
   ITG staff manages internal system accounts for all faculty, administrative staff, academic end-users and ITG privileged users.
2. Scope
   This policy is applicable to all users of Columbia Business School's computing and network resources, including offsite and collocated resources.
3. Purpose
   The purpose of this document is to provide ITG personnel with procedures they should follow when creating, modifying, and removing user directory accounts. It also details specific minimum requirements for account creation, modification and termination. Privileged accounts are also outlined here.
4. Standards for Directory Services Accounts (Microsoft Active Directory)
    a. Creating Accounts
        i. Password History
            1. Password history is enforced. Clients should be encouraged not to re-use any of the past five (5) passwords.
        ii. Password Age
            1. Maximum Password Age is enforced. Passwords will expire and have to be changed every one hundred and eighty (180) days.
            2. Minimum Password Age is enforced. Clients cannot change their password for a period of three (3) days to prevent cycling though history requirements.
            3. **Exception**: Security Incident Response policy requires password to be changed and/or reset immediately. See "Security Incident Response" for more details.
        iii. Password Length
            1. Minimum Password Length should be enforced. Passwords should be eight (8) or more characters.
                a. Administrative accounts should be no fewer than twelve (12) or more characters.
        iv. Password Complexity
            1. Minimum Password Complexity should be enforced. They should not be comprised from the principal's user name or real name, and should contain a mix of characters from at least three different character classes (uppercase, lowercase, integer, special-character)
        v. Password Protection
            1. Passwords should not be **shared** with anyone, and should be treated as company confidential information.
            2. When a machine is brought to TSG for service, a password reset is required. The TSG tech should not be required to retain the community member's password.
            3. When TSG returns a machine to a client, the password can be reset to the original password the client was using before the point-of-service.

4. Passwords **should not** be sent via email or any other un-encrypted transport.
5. Password Storage Encryption should be enforced. This mechanism is variable. Contact ITG Information Security Officer for specific recommendations.
6. Password re-use: Passwords used at Columbia Business School should not be re-used or in common with any other system (i.e. Social media, Twitter, Facebook, etc.)

vi. Account Lockout
1. Duration: 15 minutes
2. Threshold: 10 invalid logon attempts
3. Unlock Requests: CBS accounts will be unlocked by appropriate Information Technology Group support group staff pending proper identity verification. Verification should be done out-of-band (via phone and not email), and is determined by TSG staff.

vii. Account (Password) Resets
1. Verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the authentication credential is modified.

b. Managing Accounts
i. ITG – Privileged Accounts :
1. Privileged user accounts must have associated change-control ticket.
    a. Ticket should outline: user, purpose, system and expiration.
2. Unix/Linux systems
3. Administrators do not have Root accounts. Super User accounts must be approved though change control process.
4. Administrators must sudo to Root to gain Root account access
    a. All sudo requests are logged in sudoers log file
    b. Any sudo to Root that is rejected alerts appropriate ITG staff members
5. Default and vendor default administrative account passwords **must** be changed at system installation and/or configuration time.

ii. Windows systems
1. Domain Administrator access is limited to ITG infrastructure support services.
2. Administrator access is limited to ITG staff and community members that have exceptions filed with ITG
3. All account access is logged and auditable for 90 days
4. Default and vendor default Administrative Account passwords **must** be changed

iii. Service Accounts, Vendor Accounts
1. Service accounts should be created to serve a particular service function.
2. Vendor accounts will have a set expiration date to coincide with service contract renewal dates.

iv. Classification
1. Faculty & Administrative Staff
2. Student
3. Alumni
4. All other constituencies

v. Account Review
1. Accounts will be reviewed by ITG Technology Services Group(s) at least annually. Reviews will determine:
    a. Least Privilege to perform job function
    b. Employment status
    c. Academic status

2. Temporary accounts assigned to contractors, temporary workers, guests, consultants, etc.
    a. **Least Privilege to perform job function**
    b. Account expiration date **must** be provided.
3. Research Computing
    a. Accounts will be created upon request and identity verification.
    b. Cleanup is performed annually by June 30th deadline.

vi. Termination
1. Accounts of terminated individuals should be disabled/removed on a case by case basis in cooperation with Human Resources and/or the Dean's Office.
    a. All terminated accounts should be disabled within three (3) business days maximum.
2. Accounts for all "temporary" constituents should be disabled immediately after the individual's contracted date has terminated.
3. Accounts for students are terminated according to established School policy.

c. Departmental Accounts
i. Shared accounts will not be issued, without exception.
ii. Legacy shared accounts will be converted though the account creation process.

5. Revision History:

Version	Author	Date	Comments
1.1	Ryan Whitworth	12/14/12	Initial Document
1.2	Ryan Whitworth	12/17/12	Minor changes to Section 3.