**User-Account Policy**

**Purpose**

The purpose of this policy is to provide guidance about how ***<Company Name>*** will manage accounts on systems, including, but not limited to, electronic mail systems, academic and administrative file servers, and administrative databases.

**User Account Privileges & Responsibilities**

**Protection of Account Information**  
Under no circumstances should an account holder share or disclose their login and password to anyone else, including other departmental staff, faculty, or students. The third party support / services will never ask an account holder for their username and password. If an employee receives an email message claiming to be from third party support asking for this or any other confidential information, do not respond. Giving out your password will compromise your account, leaving the ***<Company Name>’s*** network vulnerable to many serious liabilities. Any account that has been compromised in this manner will have its password immediately locked without warning. To re-enable their accounts the users will have to physically present themselves at the ***<Company Name>***’s helpdesk with their identification.

**One Account Per Person**  
An individual may have multiple accounts of different types, but only a single account of any given type (e.g., a user may have a Mail account and a Windows account, but may not have more than one Mail account).

**Monitoring of Electronic Communication**

***<Company Name>*** will not monitor the content of electronic communications of its employees in most instances, nor will it examine the content of employee electronic communications or other employee electronic files stored on its systems except under ***certain*** circumstances. In this context, "electronic communications" includes telephone communications, Internet usage, phone messages, e-mail, and computer files traversing the network or stored on college equipment.

No user should have any expectation of privacy in any message, file, image, or data created, sent, retrieved, or received by use of the organization's equipment and/or access. ***<Company Name>*** has the right to monitor any and all aspects of ***<Company Name>*** owned computer systems and to do so at any time, without notice, and without the user's permission. The policy applies to all the employees.

Examples of when monitoring and/or review may occur include, but are not limited to, the following circumstances:

* Communications or files targeted by orders of a court of law or requested in accord with the Federal Freedom of Information Act.
* Internal audit review of the employee records.
* Electronic communications or files that have been inadvertently exposed to technical staff that are operating in good faith to resolve technical problems. When technical staff inadvertently see or hear potentially illegal content in communications or files, they are required to report what they have seen or heard to appropriate authorities. Otherwise, the organization expects technical staff to treat inadvertently encountered electronic communications and files of employees as confidential and not subject to disclosure to anyone.
* Routine administrative functions, such as security tests of computing systems, including password testing by system administrators to identify guessable passwords, and investigations of attempted access into systems by unauthorized persons (system administrators and other technical staff will not access employees' electronic communications or files while performing these functions).
* For security purposes, administrators may scan documents to ensure that private information is not compromised.
* Situations such as the following two examples will be specifically reviewed by and approved by the Director of Human Resources.
  + an investigation into allegations of violations of law or policy
  + an urgent need for access to business documents when an employee is unavailable

Anyone using ***<Company Name>*'s** technology resources must comply with CCA's [Acceptable Use Policy](https://technology.cca.edu/policies/acceptable-use).

**User Account Creation**

Logins are usually generated from a combination of the first letter of the first name and the last name. When that login is already in use, a number is appended to the username until unique. (e.g., asmith, asmith1 asmith2)

**NOTICE:** It is not safe to assume that a person's email address is their first initial followed by their last name. While this is currently the case for many of our users, it will become necessary to introduce more variation in the future in order to keep logins unique.

**New Employee Account Activation**  
Employee accounts are available within one week of submission of a [New Employee Technology Requisition](https://technology.cca.edu/ets-forms) form to the HR department. Access to the accounts is given during technology orientation.

**Contractor / Consultant Account Activation**  
Contractor and Consultant access is covered in the [Third Party / Contractor Access Policy](https://technology.cca.edu/policies/third-party-contractor-access-policy).

**Generic or "Role" Email Accounts**  
There are cases when it may be necessary to create role accounts. ) --> These accounts are resource intensive for he IT team as they need to be managed manually. There are better solutions for many situations that appear to require a generic account. If there isn't a better solution, generic accounts can be created as email only accounts by submitting a request to the Helpdesk and with approval by CIO.

**User Account Expiry and Deletion**

Hiring Managers are responsible for completing the [Employee Termination Technology Checklist](https://technology.cca.edu/ets-forms) form following the termination of the employees. The form should be returned to HR with the termination ***<Company Name>*** Personnel Form. All terminated employee email accounts will be disabled no later than 30 days after termination. If no form is submitted to HR, terminated employee accounts will be disabled one week from termination date. Any data in the terminated employee's network or email accounts may be removed after that time.

**Source:** <https://technology.cca.edu/policies/user-account-policy>