END USER LOGICAL ACCESS STANDARDS

PURPOSE

The purpose of the End User Logical Access Standards is to define the requirements to be followed by Brock University account holders to protect University systems and electronic data from unauthorized access.

The Standards defined below relate to computer-based access controls called logical access controls. Logical access controls protect information technology (“IT”) systems and electronic data by verifying and validating authorized users, authorizing user access to IT systems and data and restricting access (read / write / execute/ delete) according to the user’s authorization level.

DEFINITIONS

Access. The ability to do something with a computer resource. This usually refers to a technical ability (e.g., read, create, modify, or delete a file, execute a program, or use an external connection). (Reference: NIST 800-12, Chapter 17)

Authentication. Proving to a reasonable degree that a user is who they claim to be. (Reference: NIST 800-12, Chapter 17)

Authorization. The permission to use a computer resource. Permission is granted, directly or indirectly, by the application or system owner. (Reference: NIST 800-12, Chapter 17)

Least privilege. The minimum level of data, functions or capabilities necessary to perform a user’s duties. Implementation of this principle limits the potential damage resulting from accident, error or unauthorized use of an IT system.

Multifactor authentication (MFA). A security system that requires more than one method of authenticating from independent sources to verify a user’s identity.

Role-based security. The assignment of security rights to IT systems and data based on role or job function.

Separation of duties. The assignment of responsibilities such that no one individual or function has control of an entire process or complete control. Separation of duties is a technique for maintaining and monitoring accountability and responsibility for IT systems and data.

ACCOUNT MANAGEMENT

Access

All **access** to Brock systems and data, including changes to access resulting from changes in responsibility or internal transfers, must be authorized by the end-user’s supervisor or a higher authority, and the access request and authorization documented in a central repository.

The University reserves the right to determine the structure and type of usernames, passwords and / or other identifying authorization mechanisms used for logical access.

Multifactor authentication (MFA)

Access to IT systems require MFA to login.

Principle of Least Privilege

Access to IT systems and data must be granted on the principle of **least privilege**. This means that access will be granted only to systems or data that a user requires to complete their functions at the most restrictive access level necessary to perform these functions. This enhances security of the University’s IT systems and integrity of electronic data.

Brock employee account

All new employee accounts (i.e., faculty, staff) must be initiated in Human Resources (“HR”) through Workday. Each user must be provided a unique user ID.

Role-based access

Where available by system functionality, **role-based access** must be used to grant users access to the core administrative IT systems and data. Role-based access grants users access to IT systems and data based on their roles within the University, rather than granting access based on individual user. This simplifies the administration of user access rights by associating these rights with a limited number of standardized roles, and assists in maintaining the principle of least privilege.

The assignment of multiple roles to a single user which may combine to violate separation of duties requirements identified by the business / data owner is prohibited.

Account extension

An extension of an existing account requires Level 1 (“L1”) and Level 2 (“L2”) authorizations. Managers or supervisors must use the Security Access Request Form (“SARF”) for any account extension.

All academic, teaching contracts receive a six-month account extension past the contract termination date.

Change in access requirements

Additions / removals / changes of access privileges for a Brock University employee must be initiated using the SARF, and require L1 and L2 authorizations.

Internal transfer

The manager / supervisor of an employee transferring to another department is responsible for ensuring timely termination of the employee’s access pertaining to the position being vacated via the SARF. This requires L1 authorization.

Employee termination/ departure

The manager / supervisor of a resigned/departed employee is responsible for ensuring the timely termination of employee permissions via the SARF. This requires L1 and L2 authorizations.

Retiree account

A Brock University retiree is entitled to a Brock University account with access to the Brock University portal, Library, email and wireless network. The account status is changed to

"Retired" by HR; the account is then set to expire after one year.

A retiree is required to change their password every 120 days; doing so extends the account for 12 months.

Student account

Once Brock University receives a student's application from OUAC, the University acknowledges the receipt of the application via an email to the applicant. The student then must create their new account through the my.brocku.ca portal.

All Ontario student mail accounts are automatically disabled 16 months after the student's completion / departure from the last registered class.

Alumnus account

Brock University alumni maintain basic computer access after graduation. An alumnus account is limited to the portal, wireless, general access computer labs and printing.

Alumni are required to change their password every 120 days; doing so extends the account for 12 months.

Non-Brock employee account

Non-Brock employee (e.g., Faith and Life Centre, Concordia Seminary) account creation / extension / change / deletion must be initiated using the SARF and requires L1 and L2 authorizations. All such accounts must be temporary and have an expiry date.

Conference attendee account

A conference attendee account is created through a BrockDB page (a SARF is not required). These accounts expire 10 days after account creation and are limited to wireless, library journal access, general access computer labs and printing. Conference attendee accounts cannot be extended.

A conference attendee account cannot be used to access Brock University core application systems.

Guest account

A guest account is created at the Information Technology Services ("ITS") Help Desk (located in the Campus Store or the Computer Commons) with an expiry of 10 days. A guest account will only be created upon presentation by the applicant of valid government-issued identification.

A guest account has limited access based on the type of account (e.g., wireless network, Library, surveys / questionnaires, etc.).

A guest account cannot be used to access Brock University core application systems.

Vendor / contractor / third party account

A vendor / contractor / third party account requires L1 and L2 authorizations. The vendor / contractor / third party must sign a Brock University Confidentiality Agreement prior to obtaining access.

These accounts have limited access based on the type of work contracted and include by default wireless, library journal access, general access computer labs and printing.

Access by non-account holder

Access by a non-account holder to an authorized user's account must be approved by the Associate Vice President, Human Resources and the appropriate Senior Administrative Council ("SAC") member. This access must be documented in the SARF. This may be required in the event of a departure / termination of a previously authorized user.

Deletion of expired accounts

The following dictate when an obsolete account expires and subsequently when it is be deleted from Brock University systems:

Type of Account	Reason for leaving	Account expiration	Delete from AD
Faculty / Staff	Anything other than retired	Last day of employment	24 months after last day of employment
Retirees	Retired	After one year of inactivity	After 36 months of inactivity

Type of Account	Reason for leaving	Account expiration	Delete from AD
Non-Brock	End of Brock relationship	Last day of relationship with Brock	12 months after last day of relationship with Brock
Guest	Left Brock	Last day of relationship with Brock	30 days after last day of relationship
Applicant	Never registered	10 months after account activation	24 months after account activation
Student	Not registered in a course	16 months after completion of last course	30 months after completion of last course
Alumni	Graduated	After 12 months of inactivity	After 14 months of inactivity

RESPONSIBILITIES

User accountability and responsibility

No person other than those authorized shall access Brock IT systems and data.

A user account, which allows a user to access Brock IT systems and data, is provided to an individual for their exclusive use. A user is prohibited from sharing their account(s) and / or password(s) with others. An authorized user is at all times responsible and accountable for the use of their account.

Use of another user's credentials is prohibited.

All suspicious activity on an employee account must immediately be reported to the user's supervisor, who must immediately inform the ITS Help Desk.

All suspicious activity on a student's account must immediately be reported to the ITS Help Desk.

Authorizer responsibilities

Managers / supervisors must ensure that their direct reports' access to Brock's IT systems and data is granted on the principle of least privilege. This means that access must be granted only to systems and data required by the user in order to complete their functions, and must only be granted at the most restrictive access level necessary for the user to perform these functions.

Managers / supervisors must immediately notify the ITS Help Desk of any suspicious user account activity reported to them.

Management responsibilities

L1 and L2 managers / supervisors must review at least annually the access privileges of all of their direct reports and determine whether the access is still necessary and meets the requirements of least privilege.

Managers / supervisors must immediately inform ITS if changes/ terminations to user access is required (see Account Management section above).

PASSWORD MANAGEMENT

Password usage

A user must only use their Brock University password(s) within the Brock University infrastructure or University-approved / authorized Enterprise Applications or services.

Use by a user of their Brock University password for any other purpose (e.g., social media or non-Brock University applications) is prohibited.

Initial password

An initial password must expire immediately upon use and must not be re-issued or re-used. An initial password is delivered to the user by Human Resources.

Password parameters

All user access to Brock IT systems and data must be authenticated using the ITS process for authenticating users.

Campus ID passwords must contain at least 3 types of characters (lowercase, uppercase, numbers or special characters such as "!", "@", "#", etc.) and be 10 characters or more in length.

Passwords must expire every 120 days. Users are required to change their password at this point.

Passwords must not be reused.

Passwords must not contain the user’s first name, middle name, last name, email address or login ID.

Password resets

Employees

All password resets must be done in person at the ITS Help Desk or at an IT department within your faculty unless the account holder is physically unable to get to the ITS Help Desk. In such a case, the account holder must contact Human Resources.

Picture identification is required in order for the ITS Help Desk to assist the user in re-setting their password.

Users are encouraged to set up the Office 365 self-service password reset..

Students

The Registrar’s Office can reset a student password over the phone in situations where the student is physically unable to get to the ITS Help Desk.

Password masking / encryption

Screen display of passwords must be suppressed / masked. Stored passwords or passwords in transit must be encrypted.

Default vendor passwords

Default vendor passwords delivered with a system must be changed immediately upon system activation.

Compromised accounts

Employees

An employee must immediately change their password and inform their supervisor as soon as possible if the user believes or suspects that their account has been compromised.

The supervisor must inform the ITS Help Desk immediately upon such notification.

Students

A student must immediately change their password and contact the ITS Help Desk as soon as possible if the student believes or suspects that their account has been compromised.

MONITORING

Session timeouts

A user session will be locked after a pre-determined time of inactivity, until the user re-establishes access through authorization (e.g., re-entering Campus ID and password).

All core administrative systems must have a session timeout of 30 minutes for students and 30 minutes for employees.

Account locks

In order to ensure ongoing system security by allowing only authorized access, a user account will be temporarily locked after consecutive, unsuccessful login attempts.

Logs

All connection attempts are logged. Logs are maintained for reasons of security, diagnostic and account/audit requirements. Logs are available only to authorized employees and retained for a minimum of 6 months.

All access to core administrative systems must be logged.

Account Maintenance

In order to strengthen IT security, user accounts must be periodically validated. At least annually, supervisors / managers must review the access privileges of all of their direct reports and determine whether the access is still necessary and meets the requirements of least privilege. If not, the access must be changed or the account de-activated. Managers / supervisors must immediately inform the ITS Help Desk and submit the SARF.