Identity and Access Management Policy

Last review date: November 2019, version 1.0.2

Purpose

The purpose of the Bethel University Identity and Access Management Policy is to establish the requirements necessary to ensure that access to and use of Bethel University Information Resources is managed in accordance with business requirements, information security requirements, and other Bethel University policies and procedures.

Audience

The Bethel University Identity and Access Management Policy applies to individuals who are responsible for managing Bethel University Information Resource access, and those granted access privileges, including special access privileges, to any Bethel University Information Resource.

Policy

Access Control

- Access to Bethel University Information Resources must be justified by a legitimate business requirement prior to approval.
- Where multi-factor authentication is employed, user identification must be verified in person before access is granted.
- Bethel University Information Resources must have a corresponding ownership responsibility identified and documented.
- Access to confidential information is based on a "need to know."
- Confidential data access must be logged.
- Access to the Bethel University network must include a secure log-on procedure.
- Workstations and laptops must force an automatic lock-out after a pre-determined period of inactivity.
- Documented user access rights and privileges to Information Resources must be included in disaster recovery plans, whenever such data is not included in backups.

Account Management

- All employees and students must sign the Bethel University Responsible Use of Information Technology Resources before access is granted to an account or Bethel University Information Resources.
  - Employee accounts will be created by Human Resources (for staff members) and Academic Affairs (for faculty members).
  - Individuals will not receive an account until appropriate state and federal employment requirements are met including a background check.
  - Student accounts will be created following the admissions process and no sooner than 45 days before the student’s first term is scheduled to start.
  - Transcript records, FAFSA applications and communications with admissions staff over our customer relationship management service will confirm student's identity prior to being admitted as a student.
  - If identifiable information is not adequately provided, students must show their social security card along with government issued photo identification in person before being allowed to apply for any student aid.
  - Students must also have their "fee paid" for enrollment prior to being given an account and allowed to register for courses.
  - Segregation of duties must exist among Information Resource owners are responsible for the approval of all access requests.
  - User accounts and access rights for all Bethel University Information Resources must be reviewed and reconciled at least annually and actions must be documented.
  - Information Resource owners are responsible for the approval of all access requests.
  - Any accounts that have not been accessed within a defined period of time will be disabled.
  - Accounts must be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.
  - System Administrators or other designated personnel:
    - Are responsible for modifying or/and removing the accounts of individuals who change roles with Bethel University or are separated from their relationship with Bethel University.
    - 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 Bethel University IT management personnel.
Must cooperate with authorized Bethel University Information Security personnel investigating security incidents at the direction of Bethel University executive management.

Administrator/Special Access

- Administrative/Special access accounts must have account management instructions, documentation, and authorization.
- Personnel with Administrative/Special access accounts must refrain from abuse of privilege and must only perform the tasks required to complete their job function.
- Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Shared Administrative/Special access accounts should only be used when no other option exists.
- The password for a shared Administrative/Special access account must change when an individual with knowledge of the password changes roles, moves to another department or leaves Bethel University altogether.
- In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- Special access accounts for internal or external audit, software development, software installation, or other defined need, must be administered according the Bethel University Authentication Standard.

Authentication

- Personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed and implemented according to the following Bethel University rules:
  - Must meet all the requirements established in the Bethel University Authentication Standard, including minimum length, complexity and rotation requirements.
  - Must not be easily tied back to the account owner by using things like: user name, social security number, nickname, relative’s names, birth date, etc.
  - Should not include common words, such as using dictionary words or acronyms.
  - Should not be the same passwords as used for non-business purposes.
- Password history must be kept to prevent the reuse of passwords.
- Unique passwords should be used for each system, whenever possible.
- Where other authentication mechanisms are used (e.g., security tokens, smart cards, certificates, etc.) the authentication mechanism must be assigned to an individual and physical or logical controls must be in place to ensure only the intended account can use the mechanism to gain access.
- Stored passwords are classified as confidential and must be encrypted.
- All vendor-supplied default passwords should be immediately updated and unnecessary default accounts removed or disabled before installing a system on the network.
- User account passwords must not be divulged to anyone. Bethel University support personnel and/or contractors should never ask for user account passwords.
- Security tokens (e.g., Smartcard) must be returned on demand or upon termination of the relationship with Bethel University, if issued.
- If the security of a password is in doubt, the password should be changed immediately.
- Administrators/Special Access users must not circumvent the Bethel University Authentication Standard for the sake of ease of use.
- Users should not circumvent password entry with embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Bethel University IT Management.
- Application/website remembering is allowed for users.
- If a password management system is employed, it must be used in compliance with the Bethel University Authentication Standard.
- Computing devices should not be left unattended without enabling a password protected screensaver or logging off of the device.
- Bethel University IT Support password change procedures must include the following:
  - authenticate the user to the helpdesk before changing password
  - change to a strong password
  - require the user to change password at first login.
- In the event that a user’s password is compromised or discovered, the password must be immediately changed and the security incident reported to Bethel University IT support.

Remote Access

- All remote access connections to the Bethel University networks will be made through the approved remote access methods employing data encryption and multi-factor authentication for administrative access rights.
- Remote users may connect to the Bethel University networks only after formal approval by the requestor's manager or Bethel University Management.
- The ability to print or copy confidential information remotely must be disabled.
- Users granted remote access privileges must be given remote access instructions and responsibilities.
- Remote access to Information Resources must be logged.
- Remote sessions must be terminated after a defined period of inactivity.
- A secure connection to another private network is prohibited while connected to the Bethel University network, unless approved in advance by Bethel University IT management.
- Non-Bethel University computer systems that require network connectivity must conform to all applicable Bethel University IT standards, and must not be connected without prior written authorization from IT Management.
- Remote maintenance of organizational assets must be approved, logged, and performed in a manner that prevents unauthorized access.
Vendor Access

- Vendor access must be uniquely identifiable and comply with all existing Bethel University policies.
- External vendor access activity must be monitored.
- All vendor maintenance equipment on the Bethel University network that connects to the outside world via the network, telephone line, or leased line, and all Bethel University Information Resource vendor accounts will remain disabled except when in use for authorized maintenance.

References

- ISO 27002: 6, 7, 8, 9, 12, 15
- NIST CSF: PR.AC, PR.IP, PR.MA, PR.PT, DE.CM
- Bethel University Information Classification and Handling Policy
- Bethel University Disaster Recovery Policy

Waivers

Waivers from certain policy provisions may be sought following the Bethel University Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Modified Date</th>
<th>Approved Date</th>
<th>Author</th>
<th>Reason/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>October 2016</td>
<td></td>
<td>FRSecure</td>
<td>Document Origination</td>
</tr>
<tr>
<td>1.0.1</td>
<td>January 2018</td>
<td></td>
<td>Andrew Luchsinger</td>
<td>Bethel Modifications</td>
</tr>
<tr>
<td>1.0.2</td>
<td>November 2019</td>
<td>June 2020</td>
<td>InfoSec Committee</td>
<td>Committee Review</td>
</tr>
</tbody>
</table>