Information Technology Policy
9.3200
User Accounts for 3rd Party Contractors

Contents

Document Review Log

Date Reviewed	Description of Changes
9/21/2023	Initial Draft

Purpose and Scope

This policy defines the responsibilities of IT for creating user accounts for Alvernia University ("AU") 3rd Party contractors. The policy also outlines the process for requesting user accounts for Alvernia University ("AU") 3rd Party contractors. This policy:

- Defines the process for requesting user accounts for 3rd Party contractors.
- Identifies which 3rd Party contractors can have user accounts.

This policy applies to all 3rd Party Contractors who have a user account on the Alvernia domain and the Alvernia University employees who sponsor their user accounts.

Responsibilities

Title or Role	Definition and What They are Responsible For
Chief Information Officer	Maintains and enforces this policy. Receives exceptions to the policy.
Senior Leadership Policy Committee	Serves as final approval for policy and assists with reviewing exceptions to the policy.
3rd Party Contractor with user account	Non-Alvernia employees who have normal or elevated level of access to AU network or systems. These individuals have responsibility to perform certain tasks on behalf of Alvernia University as outlined in their contract with AU. They also have significant security responsibilities. These individuals have security responsibilities as outlined in *9.3000 IT Security for IT and Data Professionals* and *9.4000 IT Security for 3rd Party Partners and Providers*.
Sponsor	Alvernia employee who is also a department leader. This individual will be responsible for requesting an account for the 3rd Party Contractor and is also responsible for notifying IT when that contractor separates from AU.

Policy

When 3rd Party Contractors need a user account or access to any AU Information Technology systems, a department leader who is an AU employee must sponsor them. Sponsors must request access for this 3rd Party Contractor from IT and must also notify IT when the contractor separates from AU. Access granted to the 3rd Party Contractor will be based upon least privilege access guidelines. If the 3rd Party Contractor does not have a need for account access, it will not be

granted. Sponsored accounts will be reviewed quarterly by IT and the corresponding Sponsors. Off-campus access to sensitive systems will require the use of Multi-Factor Authentication (MFA).

Policy Procedure

To request a sponsored account for a 3rd Party Contractor, the Sponsor should submit an email request to servicedesk@alvernia.edu with the following information:

- Contractor's full name:
- Contractor's title:
- Contractor's address:
- Contractor's phone #:
- Business requirements that warrant the need for a user account:
- What specific access is needed for this account (i.e. email, Portal, PowerCampus, etc. – be as specific as possible):
- Time period that the account is needed for (i.e. 1 week, 30 days, period of contract, beginning\ending):
- Can this access be limited to a single computer? If so, a specific computer name or asset tag number should be stated.

Once this request is received, IT personnel will validate the request and process it in a timely manner. Note that IT personnel may reach out to the Sponsor for clarification or with questions/concerns. IT will also reach out in an encrypted email to the Sponsor for contractor's DOB and last (4) of SSN. This information is entered into PowerCampus and is used by ServiceDesk personnel for password resets.

Exceptions to Policy

Exceptions to this policy must be requested in writing by filling out the Policy Exception form and submitting it to the individual named in the Responsibilities section who assists with reviewing exceptions to this policy.

Policy Review

The Information Technology policies should be reviewed on a 3-year cycle and updated when institutional needs or goals change.

References and Related Policies

This section contains any 3rd party standards, guidelines, or other policies referenced by this policy.

Related Policies

1. 9.3000, IT Security for IT Professionals
2. 9.4000, IT Security for 3rd Party Partners and Providers

Exhibits

This section contains links to any documents that are required to be used by the policy. Examples would include required forms or links to internal websites or systems required to implement the policy.

Exhibit A	Approval of IT Policy Exception
Exhibit B	Acknowledgement of Review of 9.3000

Exhibit A – Approval of IT Policy Exception

Requestor:	
Date Requested:	*Date of request. The approval date is below in the signature section*
Policy reference:	*Specific policy section to which an exception is being requested*
Description of systems or applications impacted:	
Rationale for the exception:	*Options may include lack of support from underlying technology. If there are any compensating controls, these should be noted here.*
Business Risk:	*A discussion of the potential impact to confidentiality, integrity or availability of the systems or applications goes here.*
Approved By:	
Title:	*Per policy, this should always be the Chief Information Officer*
Date Approved:	

Exhibit B - Acknowledgement of Review of 9.3000

The language below shall be used to acknowledge review and acceptance of the 9.3000 policy by IT and Data Professionals.

Subject: Acknowledgement of Review 9.3000

I acknowledge that I have reviewed **9.3000, IT Security for IT and Data Professionals**, understand my responsibilities as outlined therein, and agree to comply to the best of my ability. I also understand that failure to comply with AU security policies may result in disciplinary action.

Name: _____

Signature: _____

Date: _____