

Miami University

Third Party Elevated Privilege Remote Access Standard

IT Policy | **IT Standard** | IT Guideline | IT Procedure | IT Informative
Issued by: IT Services

SCOPE:

This standard covers the requirements placed on third parties when remotely accessing Miami University systems with credentials that provide elevated privileges for purposes other than collaborating on research. This standard also covers the responsibilities of Miami users who have provided access to a third party and of the Security Engineering team within IT Services.

RATIONALE:

Setting security standards for remote access of systems by third parties increases Miami's overall security posture. Regular review by the sponsoring department of actions taken by sponsored third parties on Miami's systems help ensure that the access is appropriate. This improves both the security of Miami systems and of the data contained therein.

IT STANDARD:

A. Obtaining initial access

To obtain the ability to remotely access Miami systems, the third party must be sponsored by an individual employed by Miami. This employee or their designee ("the sponsor") will contact the Security Engineering group within IT Services to request initial access for the third party. The sponsor will provide all information requested by the Security Engineering group to process this request. This includes a completed and signed copy of the Miami Services Agreement document.

B. Obtaining ordinary access

After initial access has been provided, the third party must request ordinary access to create a time frame in which they can access Miami systems remotely. The third party must contact the sponsor for this. The sponsor is the only person who is able to grant ordinary access to the third party. Security Engineering has no involvement in providing ordinary access.

C. Requirements for third party access

All access of Miami systems must be done in accordance with the Responsible Computing Use Policy and with the Confidential Information Policy. Both policies are available for review in the [Miami University Policy and Information Manual](#). Any access to a system containing payment card data must be in conformance with the Payment Card Industry Data Security Standards (PCI DSS). Any access to any system containing information governed by laws or regulations, especially the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm Leach Bliley Act (GLBA) and Ohio Revised Code chapter 1347, will be in conformance with those laws and regulations.

D. Responsibilities of the third party

Each third party will be provided with a unique user ID and password. This user ID and password cannot be shared with anyone, including other employees of the same company. If additional employees of the same company require access, they will work with their sponsor to obtain this access.

For both initial access requests and ordinary access requests, the third party will contact their sponsor.

When ordinary access is required, the third party is responsible for following the ordinary access request procedure in the appendix for the acceptable method of remote access that they are using. A total of three simultaneous connections will be allowed per ID. The third party is responsible for ensuring that their actions are in accordance with the requirements listed above.

E. Responsibilities of the sponsor

The sponsor is responsible for forwarding initial access requests from the third party to Security Engineering. The sponsor is also responsible for approving ordinary requests from the third party.

The sponsor is responsible for regularly reviewing the logs of the third party's activities on Miami systems. This review includes confirming that access by the third party is in accordance with the requirements listed above. The sponsor is also responsible for contacting the IT Services administrator who normally maintains the server of the times when the server may be accessed by the third party.

F. Responsibilities of the Security Engineering

Security Engineering (SE) will work with the sponsor to process initial requests. SE is not responsible for processing ordinary requests, as those are the responsibility of the sponsor.

SE will, when requested, provide the sponsor with training in how to access and review logs. SE will, when appropriate, work with the sponsor and the third party to troubleshoot connectivity issues.

G. Methods of remote access

Only methods of remote access listed in the appendix may be used. No other methods of third party elevated privileged remote access for purposes other than collaborating on research are approved.

H. Exceptions

Any exceptions to this standard require approval from the Information Security Officer before they are implemented.

I. Review

This standard will be reviewed by the Information Security Officer on an annual basis.

APPENDIX:

Acceptable methods of remote access eGuardPost

Ordinary access request procedure Using eGuardPost

1. The third party accesses the eGuardPost website to request the system that they need to access, as well as the time and date of the access and the size of the access window. The access window only controls when the session can be initiated, not the duration of the session. Access continues uninterrupted as long as the third party is active in the session. Access windows cannot be longer than 24 hours.
 - a. Example - If a third party requests an access window from 4 – 8 PM, they can log in and out multiple times within that window. If they login at 7 PM and have 4 hours of work to perform, the session will continue as long as the third party remains active. Once they logout outside of the access window, they will need to request access again.
2. After the third party requests access, eGuardPost will automatically send an email to all individuals listed as approvers for that system. The approvers are defined during the initial access configuration, and are typically the application owners. Any individual who receives this email can allow the third party access to the system.
3. Once an approver has approved the request, the third party will receive email indicating the access window that is available for accessing the system.

DEFINITIONS:

Initial access – The configuration of an account for a third party on the remote access system.

Ordinary access – Access for a third party through the remote access system to a Miami system maintained or configured by the third party.

Third party – Any individual who does not have a Miami Unique ID or a Miami Courtesy Account.

APPROVAL(S) AND DATE(S):

Reviewed by: Security Engineering, May 13, 2009

Final Approval by: IT Services Leadership Team

Final Approval on: May 26, 2009

Version number: 1.0

REVISION HISTORY & REFERENCES:

- A. Revision History
May 26, 2009 – First Draft