Mizuho Securities USA Inc.

Mizuho IT: Policies and Procedures

Vendor Remote Access

Document Version

Author / Editor	Change	Date	Version
McGlashan, James	Initial Draft	04/17/13	0.01

Table of Contents

1 Introduction

1.1 Purpose and Scope

This document describes the Mizuho Securities USA policies and procedures relating to managing remote access to Mizuho IT resources by vendors. To protect Mizuho Securities USA information from unauthorized access, use, and disclosure by providing guidelines for appropriate vendor remote access.

Mizuho Securities USA relies on the services of Vendors to complete several support functions. Vendors pose security risks that exceed those of other users. Vendors, for example, may not benefit from the system controls, and policy restrictions imposed on Mizuho Securities USA systems and employees. Therefore, remote access privileges for vendors require additional review and a high degree of trust with the third party.

Vendor remote access to Mizuho Securities USA systems should only be granted to perform specific functions. Vendors will be granted remote access into the Mizuho Securities USA network only if required to perform maintenance, troubleshooting, upgrades, or monitoring. Access should be limited to the specific server(s) and communications mechanisms (Shared session, SSL VPN, Modem, etc.) which are the minimum necessary to perform the required support.

1.2 Audience

This document is meant to be read and understood by all Mizuho Securities USA IT employees and managers or employees who have authority with the vendor are responsible to request and monitor access for them.

1.3 Definitions, Acronyms and Abbreviations

The following terms and abbreviations are used throughout this document.

Term	Meaning
MSUSA	Mizuho Securities USA Inc.
Vendors	Vendors or third parties providing MSUSA with consulting, support, diagnostic, monitoring, or one of many other services where the service is provided remotely. Specifically where providing the service involves access of MSUSA systems and or applications from vendor systems or applications. Consultants or contractors working solely on MSUSA systems are addressed under the MSUSA Account Management Policy.
Remote Access	Accessing MSUSA systems by people or systems external to the MSUSA network.
Access Sponsor	Application owners or other parties who have authority with the vendor and are requesting access to MSUSA systems for the vendor.
Shared Account	Accounts that are shared by more than one user or shared by a system and a user.
Privileged Account	Accounts that have more privileges than a normal user. Examples include, root, accounts with unrestricted sudo, accounts with local or domain administrator roles.
IDS	Intrusion Detection System. Monitors network activities for malicious activities or policy violations.

2 Policies

2.1 Vendor Access Types

Vendor access types should be viewed in one of the following primary categories.

2.1.1 Shared Session

The preferred method for intermittent or infrequent vendor access to MSUSA systems is via web-based Juniper Meeting Secure Gateway (https://remoteoffice.mizuhosecurities.com/) or an equivalent service (i.e. WebEx, GoToMeeting, etc).

- The activity is under the control and supervision of a MSUSA employee and does not require a vendor account.
- Vendors must be limited to access only to the systems required (i.e. email and unnecessary applications must not be shared)
- Data is transmitted via an SSL web connection (https://) which ensures that data sent over the connection is encrypted.

2.1.2 Internet Access

An alternative method for infrequent vendor access to MSUSA systems is via the Juniper SSL VPN.

- Vendor SSL VPN accounts must have an approved Vendor account request.
- Vendor SSL VPN accounts must be secured with RSA two factor authentication.
- All VPN connections must be logged.
- All VPN firewalls must be logged.
- All VPN network activity must be monitored by the MSUSA IDS platform.
- Vendors requiring network level remote access will be limited to connect only to the systems they require.
- Access to systems will require an approved access request.
- Data is transmitted via an SSL web connection (https://) which ensures that data sent over the connection is encrypted.

2.1.3 Modem Connection

Where systems do not support network based remote access, a modem may be requested.

- Access to the system should be password controlled.
- If the system cannot support password control on modem access, it is acceptable to use password restriction in the modem.
- If there is no ability to require password access control the modem should only be connected when required for support activity.
- Modems connected to MSUSA systems will be audited annually.

2.1.4 Dedicated Connection

Where dedicated or frequent vendor access to MSUSA systems is required, limited network peering either through VPN or private line may be requested.

- Vendor dedicated connection must have an approved network peering request.
- Connections must terminate in a DMZ where access can be limited to approved devices and protocols.
- All VPN connections must be logged.
- All VPN firewall events must be logged.
- All VPN network activity must be monitored by the MSUSA IDS platform.
- Vendors requiring network level remote access will be limited to connect only to the systems they require.
- Access to systems will require an approved access request.
- Where possible all activity should be logged.
- Dedicated connections to MSUSA systems will be audited annually.

2.2 Vendor Account Types

2.2.1 Unique Accounts

Vendor accounts are considered unique when only one Vendor has the authentication credentials for the account. Accounts are not to be shared between vendors or a vendor and MSUSA employees.

- Vendors should use unique login accounts per system.
- Vendor login accounts should be disabled when not in use.
- Login accounts should be maintained in Active Directory where possible.
- Vendor accounts must be limited to the systems required to be supported.
- Where Active Directory accounts are not possible local accounts may be added to the specific systems required to be supported.

2.2.2 Shared Accounts

Accounts are considered shared when both MSUSA and the Vendor have the authentication credentials for the account.

- Accounts with authentication credentials shared between MSUSA and Vendors require an IT exception.
- Vendors should not have access to any MSUSA user or administrative accounts.
- Vendors must access shared accounts through a jump machine where access and activity can be logged.

2.3 Provisioning Remote Access

- Accounts will be requested following the Mizuho IT Account Management Policy.
- All MSUSA owned assets (except two factor tokens) will be tracked as per the MSUSA Asset Management Policy

2.4 Termination of Remote Access

- Upon termination of the contract, agreement or other arrangement, remote access will be terminated.
- All MSUSA assets, including two factor tokens, must be returned to MSUSA IT.
- In the case where the account credentials are shared, and the account cannot be removed or changed, the account password must be changed.
- Returned asset tracking will be updated as per the MSUSA Asset Management Policy

2.5 Vendor Devices

- Vendors shall not connect any type of hardware to the internal Mizuho network or systems without prior authorization and under the direction and supervision of Mizuho IT personnel.
- Vendors shall not connect any type of storage device i.e. flash drive, CD-ROM, external hard drive, or any other removable media to any Mizuho device or network, without prior authorization and at the direction and supervision of Mizuho IT personnel.
- In the event that a vendor has software, updates or other data that must be transferred to the internal network or systems, the data should be provided to a Mizuho IT to be scanned for malware.

3 Monitoring

- All remote access sessions are subject to monitoring.
- Login/Logoff Login date, time, and username must be recorded by the systems accessed.
- Login access failures date, time, and username must be recorded by the applications accessed.
- All keystrokes and system activity should be logged.
- Remote access logs should be correlated with account access logs.

4 Procedures

4.1 Vendor Account Requests

Vendor Remote Account Requests are to follow the Mizuho User Account Management Policy.

4.2 Vendor Onboarding

The following information is required for a successful Vendor Remote Access onboarding effort.

1. Application
   - What application of system requires vendor remote access?
2. Business sponsor.
   - Who is the MSUSA sponsor for the vendor access?
3. Vendor access requirements.
   - What is the Vendor technical point of contact for implementation and operational issues?
   - What access methods are required?
   - Which servers require access?
   - What accounts are required per server?
   - What privilege is required per accounts per server?
4. Firewall access requests
   - Source IP address, Destination IP address, Protocol, Port
5. IDS monitoring request
   - List of required protocols and destinations.
6. Grant access to approved systems
   - Are Courion Requests submitted and approved?
7. Validate access and logging
   - Verify application log data is being reporting in centralized log system.

5 Compliance and Review

The following review steps will be taken – periodically or according to the stated frequency – to help ensure compliance with the stated goals of this document:

Step	Frequency	Responsible
Vendor Remote Access account activity review.	Quarterly	Governance
Vendor account management policies and procedures.	Annually	Governance
Audit active vendor firewall requests.	Annually	Governance
Audit modems connected to MSUSA systems.	Annually	Governance
Audit dedicated connections to MSUSA systems.	Annually	Governance

6 Appendix

6.1 External References

6.1.1 User Account Management Policy

K:\Policies\IT\MizuhoIT_Policy_UserAccountManagement.pdf

6.1.2 User Authorization form (Courion)

http://shobcriownprd01/AccessRequestPortal/admin/adminviewrequest.aspx

6.1.3 Asset Management Policy

K:\Policies\IT\MizuhoIT_Policy_AssetManagement.pdf

6.1.4 Accounting Fixed Assets Process

K:\Accounting\AssetSpreadsheet\Accounting Fixed Assets Process v3.doc

6.1.5 Account Authorization Policy

K:\Policies\IT\MizuhoIT_Policy_UserAccountManagement.doc