HOW MX PROTECTS YOUR DATA
Overview

MX is passionate about and dedicated to protecting, safeguarding, and securing customer data. To do so, MX has established a strong security program supported by a comprehensive suite of security, confidentiality, and privacy policies, processes, procedures, and security controls. This security whitepaper highlights MX’s security approach to each of the following areas:

1. **Security Governance**
   - Security Strategy, Program, and Policies
   - Risk and Vulnerability Management
   - Incident Response

2. **Physical Security**
   - Physical Access and Environmental Protection

3. **System Security**
   - Logical Access Control
   - Network Security
   - System Hardening, Baselines, and Configuration Management
   - Logging, Monitoring, and Alerting
   - Segregation of Duties
   - System Resiliency, Business Continuity, and Disaster Recovery

4. **Application Security**
   - Code Security and Change Management

5. **Data Security**
   - Data Classification, Handling, and Encryption
   - Data Leakage Protection

6. **Personnel Security**
   - Human Resources Security
   - Security Awareness

7. **Third Party Security**
   - Third Party Vendor Risk Management
   - Assurance Reports
1. SECURITY GOVERNANCE

As noted above, OS baselines and associated system configurations, code repositories, and identified and execute corrective changes. The MX Information Security team has defined critical security alert criteria. These are applied to each risk and are calculated based on both the impact and likelihood of untested or potentially malicious code being deployed to production.

MX systems are hardened using industry-recognized hardening standards and reported by this centrally managed deployment mechanism. System, database, and application activities are logged and monitored for irregular and inappropriate access to systems and user permissions are reviewed on a periodic basis.

User access to systems and user permissions are reviewed on a periodic basis. Privilege by provisioning only the needed permissions to users in order to perform their job function. MX personnel are encouraged and required to pass a robust background check prior to starting employment at MX. As part of this awareness instruction to these personnel, MX maintains compliance with the security awareness training. This training is provided as a refresher to MX personnel on a regular basis. Any blockers identified in risk mitigation activities are provided to MX’s Incident Response Plan.

MX relies on secure data center colocation facilities to house MX infrastructure including, but not limited to, data center physical security, logical access control, assurance reports, and third-party security. MX systems are hardened using industry-recognized hardening standards. Part of MX’s security program includes a continuous risk and vulnerability management process. MX enacts defense in depth by hardening each layer of MX’s infrastructure and supporting processes.

MX personnel are required to wear their MX identification (or I.D.) badge in a manner that prevents removal and unauthorized access to MX corporate office doors—protected against direct or inadvertent modification. MX personnel are required to pass a robust background check prior to starting employment at MX. As part of this awareness instruction to these personnel, MX maintains compliance with the security awareness training. This training is provided as a refresher to MX personnel on a regular basis. Any blockers identified in risk mitigation activities are provided to MX’s Incident Response Plan.
Security Governance

Security Strategy, Program and Policies

MX’s approach to security includes a defense-in-depth strategy. This strategy is supported by an established, operational MX Security Program, with a robust suite of supporting policies, processes, security controls, and procedures to achieve MX’s security strategy. MX enacts defense in depth by hardening each layer of MX’s infrastructure and supporting processes.

Risk and Vulnerability Management

MX deploys a defense-in-depth security model—securing MX systems against malicious attacks at each level and layer. To proactively identify potential risks, MX deploys several vulnerability and risk detection mechanisms including, but not limited to, continuous security vulnerability scans, conducts regular compliance and security audits, reviews security alerts, and engages third-party assessment organizations to conduct rigorous external penetration tests.
Results of these risk detection activities are consolidated and input into MX’s Risk Management dashboard. The MX Risk Management dashboard is reviewed by the Head of Information Security on a regular basis—accounting for updated scan results, audit findings, Security Information and Event Management system (SIEM) event reviews, system security alerts, and other information collected on a regular basis. Risk ratings are applied to each risk and are calculated based on both the impact and likelihood of each risk. MX’s Information Security team creates risk mitigation plans for each risk and executes these risk mitigation plans. Status of risk mitigation activities contained within MX’s Risk Management dashboard are communicated to MX’s management team on a regular basis. Any blockers identified in risk mitigation activities are provided to MX’s management team in order to diffuse any risk mitigation disrupters in a timely manner.

**Incident Response**

MX’s Information Security team has established, maintains and executes, as needed, the MX Incident Response Plan. MX’s Incident Response Plan includes criteria for when the MX Incident Response Plan should be executed, procedures for how to effectively facilitate incidents, and processes for communicating incident details (when customer impacting) to customers. The MX Incident Response Plan is reviewed, updated (as needed), and tested on an annual basis.

MX’s Information Security team provides a mechanism for MX personnel and external system users to report potential security incidents. MX personnel are encouraged and trained to report security-related incidents directly to MX’s Information Security team either verbally, via internal communication mechanisms, or by emailing security@mx.com.

External system users are able to report security-related incidents via clicking the “Contact Support” links available in MX’s applications, contacting their MX customer service representative, or by emailing security@mx.com.
2
PHYSICAL SECURITY
Physical Security

Physical Access Control and Environmental Protection

Data Centers

MX relies on secure data center colocation facilities to house MX infrastructure including, but not limited to, buildings, power (including redundant power supplies, UPS, and generator backup power), HVAC (including temperature and humidity controls), racks, and system components (including network devices and servers).

MX equipment is isolated in secured partitions in each data center colocation facility. Partitions are built with tamper-resistant hardware and extend from subfloor to partition ceiling.

Physical access to these locations is provided to authorized personnel only. Physical access to these locations does not provide logical access to systems (for logical access to systems, see Logical Access Control). Physical access to data center colocation facilities is granted to authorized persons via electronic key card having the appropriate access permissions and either PIN or biometric authentication. Cameras are in place to monitor ingress into the data center colocation facilities. Physical access lists are reviewed on a periodic basis for appropriateness, and physical access is removed when MX personnel terminate their employment for any reason.

Visitors to data center colocation facilities require authorization by designated MX personnel. Visitors check into the data center colocation facility upon arrival. Each visitor’s identity is authenticated using a government-issued identification. Visitors are escorted at all times by authorized MX personnel.

Data center colocation facilities are required to maintain compliance with the AICPA’s Trust Services Principles and Criteria (TSP), and provide evidence indicating ongoing compliance with the TSP by providing a Report on the Design and Operating Effectiveness of Controls at Service Organizations (SOC-2 Type II Report) issued by a third party assessment organization.
Office Buildings

Physical access to MX corporate office buildings is secured to allow only MX personnel with an active electronic key card. Physical access is removed when MX personnel leave MX. Physical access control lists are reviewed periodically for appropriateness. MX personnel are required to wear their MX identification (or I.D.) badge in a manner that allows others to easily see. The MX identification (or I.D.) badge has no logos or other information that would attribute the badge to the MX corporate office building.

Visitors to MX corporate office buildings check in at the reception desk. Each visitor’s identity is authenticated using a government-issued identification. Visitors are required to sign in using the visitor access log prior to being provided a visitor badge. The visitor badge is a card that does not have the ability to enter through MX corporate office doors. Visitors are escorted at all times by authorized MX personnel.
How MX Protects

Awareness training, MX personnel are instructed to report any suspicious behavior to. As part of MX’s new hire orientation, new hires are provided a thorough information compliance processes are embedded into MX’s culture, and are demonstrated by the MX personnel are trained and educated to be assertively securit. Security Awareness employment.

with appropriate consequences, including disciplinary action up to termination of personnel. MX personnel found not adhering MX Policy are subject to investigation Security team provides role-based security-related training and MX personnel are required to pass a robust background check prior to starting employment.

Vulnerability and risk detection mechanisms including, but not limited to, continuous infrastructure and supporting processes. Risk and Vulnerability Management

MX enacts defense in depth by hardening each layer of MX’s security strategy. MX enacts defense in depth by hardening each layer of MX’s supporting policies, processes, security controls, and procedure.

To ensure the organization and each change, a peer review, systematic code style checks, code security review (including repository. Changes to software repositories require a documented description of the change, a peer review, systematic code style checks, code security review (including repository. Changes to software repositories require a documented description of the change, a peer review, systematic code style checks, code security review (including repository. Changes to software repositories require a documented description of the.

Logical access to MX production system components is limited to MX personnel. Visitors are escorted at all times by authorized MX personnel. Visitors check into the data center colocation facility upon arrival. Each MX personnel terminate their employment for any reason. MX equipment is isolated in secured partitions in each data center colocation facility.

Third Party Security

In order to support MX’s Business Continuity Plan, MX has a Disaster Recovery Plan (DRP) that includes detailed plans for restoration of systems and system configurations in the event of catastrophic system failure. As noted above, OS baselines and associated system configurations, code repositories, impact impactful system outages.

MX production systems are architected with the level of resiliency required to meet deployment of code to production systems are performed by separate people. Development of code takes place in the development environment. Testing of Segregation of Duties

criteria are applied to monitoring systems to produce alarms and notifications, which are The MX Information Security team has defined critical security alert criteria. These authoritative NTP time sync sources to help ensure events and logs are using.

format—protected against direct or inadvertent modification. S...
**System Security**

**Logical Access Control**

Logical access to MX production system components is limited to only authorized personnel with a legitimate business justification and documented engineering, operations, or security management approval. MX follows the principle of least privilege by provisioning only the needed permissions to users in order to perform his/her job function.

Users are authenticated to the MX production environment using strong multifactor authentication mechanisms that include a complex password and one-time passcode authentication token. Passwords are rotated on a quarterly basis.

User access to systems and user permissions are reviewed on a periodic basis. User access is removed from MX systems when personnel leave MX.

**Network Security**

Network devices are configured to use secure configurations. Network device firmware are kept up-to-date by applying the latest patches provided by network device manufacturers.

Firewalls are configured to deny all traffic except permitted by justified exception. Firewall rules are periodically reviewed to help ensure rule sets are configured to limit ingress and egress communications to only those required for the operations of MX services.
System Hardening, Baselines, and Configuration Management

MX systems are hardened using industry-recognized hardening standards such as Defense Information Systems Agency (DISA), Security Technical Implementation Guide (STIG) and Center for Internet Security (CIS) benchmarks. A baseline Operating System (OS) image is used for every system build.

Patches are applied to systems in a timely manner. Patching includes updating the baseline OS image for all new builds and also includes updating systems currently running in production. As part of the patch application process, MX strategically applies updated patches (including major version changes) to systems in a pre-production environment for testing and system analysis. When testing is complete in a pre-production environment, patches are applied to systems, in a methodical way, to systems in the production environment.

OS configurations are orchestrated by centrally managed deployment mechanisms. Configurations are pushed out to systems on an ongoing basis to help ensure systems maintain baseline configurations. System configuration deviations are identified, logged, and reported by this centrally managed deployment mechanism.

The OS baseline and associated system configurations are regularly backed up to help ensure timely restore of systems and system configurations in the event of catastrophic system failure.

Logging, Monitoring, and Alerting

System, database, and application activities are logged and monitored for irregular and otherwise suspect system and user behaviors. Logs are sufficiently detailed to support MX’s incident response and root cause analysis processes. Logs are in read-only format—protected against direct or inadvertent modification. Systems sync with authoritative NTP time sync sources to help ensure events and logs are using accurate time stamps.

The MX Information Security team has defined critical security alert criteria. These criteria are applied to monitoring systems to produce alarms and notifications, which are sent to the MX Information Security team to review, investigate, determine root cause, and identify and execute corrective changes.
Segregation of Duties

MX segregates its development, Quality Assurance (QA), and production environments—both via network segmentation and logical access restrictions. Development of code takes place in the development environment. Testing of pre-production builds take place in the QA environment. Production code, after appropriate authorization, is deployed into the production environment.

In addition to segregating application environments, MX also segregates request, approval, and provisioning duties as part of both the logical access request process and the change deployment process. Requests for, approvals of, and provisioning access to production systems are performed by separate people. Additionally, approval and deployment of code to production systems are performed by separate people. Segregating duties in these critical processes is key to reducing the risk of fraud, error, and other potential malicious activities.

System Resiliency, Business Continuity and Disaster Recovery

MX production systems are architected with the level of resiliency required to meet operational up-time requirements. MX operates using 2N (redundant) production environments. Each production environment is located in geographically separate, fault-tolerant zones—significantly reducing the likelihood of full system failure and impactful system outages.

As noted above, OS baselines and associated system configurations, code repositories, and critical system data are regularly backed up to help ensure timely restoration of systems and system configurations in the event of catastrophic system failure.

MX maintains a Business Continuity Plan that identifies business impacting systems and processes, critical dependencies, and strategy plans to restore business operations in the event of a business impacting event.
In order to support MX’s Business Continuity Plan, MX has a Disaster Recovery Plan that lists and describes critical system components, identifies recovery time and point objectives, and contains procedures to recover from a catastrophic system failure. MX’s Disaster Recovery Plan is reviewed, updated (as needed), and tested on an annual basis.
compliance processes are embedded into MX’s culture, and are demonstrated by the appropriate consequences, including disciplinary action up to termination of personnel. MX personnel found not adhering MX Policy are subject to investigation.

vulnerability and risk detection mechanisms including, but not limited to, continuous infrastructure and supporting processes.


Security Governance

Code deployment is limited to only authorized software development personnel. Additionally, authentication to these zones is via interface tools that restrict access to the office environment.

Visitors to MX corporate office buildings check in at the reception desk. Each visitor’s identity is authenticated using a government-issued identification. Visitors are provided a visitor badge and are required to sign in using the visitor access log prior to being provided a visitor badge. The visitor’s identity is authenticated using a government-issued identification. Visitors are provided a visitor badge and are required to sign in using the visitor access log prior to being provided a visitor badge.

MX personnel are required to wear their MX identification (or I.D.) badge in a manner that lists and describes critical system components, identifies recovery time and point objectives, and contains procedures to recover from a catastrophic system failure. MX equipment is isolated in secured partitions in each data center colocation facility. Physical access control lists are reviewed periodically for appropriateness. MX segregates its development, Quality Assurance (QA), and production environments.

Segregation of Duties

Development of code takes place in the development environment. Testing of deployed code on that single node and, when confirmed successful on the testing environment, a peer review, systematic code style checks, code security review (including checks against OWASP’s Top 10 common coding vulnerabilities and other code vulnerabilities), and third party security review is performed on the third party prior to using third party services. As part of the security review, identified findings are discussed with and provided to the third party to remediate within an agreed-upon timeframe. MX engages qualified third party assessment organizations to audit third parties on an annual basis. Identified findings are discussed with and provided to the third party to remediate within an agreed-upon timeframe.

MX provides evidence indicating ongoing compliance with PCI DSS as updated on an annual basis. These compliance reports can be provided to MX services representative, or by emailing security@mx.com.

Please direct any questions to the MX Information Security team. MX invests heavily in reducing security risks at each layer of its organization and each process. MX’s Disaster Recovery Plan is reviewed, updated (as needed), and tested on an annual basis. A comprehensive suite of security, confidentiality, and privacy policies, processes, procedures, and security controls. This security whitepaper highlights MX’s security policies and procedures. Additional information can be found at www.mx.com/about/privacy.

Overview

Segregating duties in these critical processes is key to reducing the risk of fraud, accidental errors, and other risks. The MX Information Security team has defined critical security alert criteria. These alerts are prioritized based on the impact to the system and the organization.

System, database, and application activities are logged and monitored for irregular and unusual patterns. Configurations are pushed out to systems on an ongoing basis to help ensure systems are hardened using industry-recognized hardening standards. MX systems are hardened using industry-recognized hardening standards, including *System, database, and application activities are logged and monitored for irregular and unusual patterns.*

MX’s Disaster Recovery Plan is reviewed, updated (as needed), and tested on an annual basis. A comprehensive suite of security, confidentiality, and privacy policies, processes, procedures, and security controls. This security whitepaper highlights MX’s security policies and procedures. Additional information can be found at www.mx.com/about/privacy.

System Security

MX’s Disaster Recovery Plan is reviewed, updated (as needed), and tested on an annual basis. A comprehensive suite of security, confidentiality, and privacy policies, processes, procedures, and security controls. This security whitepaper highlights MX’s security policies and procedures. Additional information can be found at www.mx.com/about/privacy.

Incident Response

MX’s Disaster Recovery Plan is reviewed, updated (as needed), and tested on an annual basis. A comprehensive suite of security, confidentiality, and privacy policies, processes, procedures, and security controls. This security whitepaper highlights MX’s security policies and procedures. Additional information can be found at www.mx.com/about/privacy.

Risk and Vulnerability Management

MX’s Disaster Recovery Plan is reviewed, updated (as needed), and tested on an annual basis. A comprehensive suite of security, confidentiality, and privacy policies, processes, procedures, and security controls. This security whitepaper highlights MX’s security policies and procedures. Additional information can be found at www.mx.com/about/privacy.

Logging, Monitoring, and Alerting

MX’s Disaster Recovery Plan is reviewed, updated (as needed), and tested on an annual basis. A comprehensive suite of security, confidentiality, and privacy policies, processes, procedures, and security controls. This security whitepaper highlights MX’s security policies and procedures. Additional information can be found at www.mx.com/about/privacy.

Applying and Monitoring Security Policies

MX’s Disaster Recovery Plan is reviewed, updated (as needed), and tested on an annual basis. A comprehensive suite of security, confidentiality, and privacy policies, processes, procedures, and security controls. This security whitepaper highlights MX’s security policies and procedures. Additional information can be found at www.mx.com/about/privacy.

Security Awareness

MX’s Disaster Recovery Plan is reviewed, updated (as needed), and tested on an annual basis. A comprehensive suite of security, confidentiality, and privacy policies, processes, procedures, and security controls. This security whitepaper highlights MX’s security policies and procedures. Additional information can be found at www.mx.com/about/privacy.

Third Party Security

MX’s Disaster Recovery Plan is reviewed, updated (as needed), and tested on an annual basis. A comprehensive suite of security, confidentiality, and privacy policies, processes, procedures, and security controls. This security whitepaper highlights MX’s security policies and procedures. Additional information can be found at www.mx.com/about/privacy.
Application Security

Code Security and Change Management

Application code is managed and deployed using a centrally managed software repository. Changes to software repositories require a documented description of the change, a peer review, systematic code style checks, code security review (including checks against OWASP’s Top 10 common coding vulnerabilities and other code vulnerability checks), and approval from a software engineering development lead.

Code is deployed to servers in a methodical manner—deploying code to a single node, testing the deployed code on that single node and, when confirmed successful on the single node, code is then deployed to all subsequent nodes.

Code deployment is limited to only authorized software development leads. By limiting access to only a select set of individuals with the ability to deploy code reduces the likelihood of untested or potentially malicious code being deployed to production systems.

Code repositories are regularly backed up to help ensure timely restore of applications in the event of catastrophic system failure.
Our Data Security team provides role-based security-related training and employment at MX. Job roles and responsibilities are communicated to MX personnel. MX deploys a defense-in-depth security model—securing MX systems, environments, and processes. This includes the deployment of security software, the implementation of network security measures, and the execution of vulnerability and patching strategies. Our approach ensures the security of MX systems by supporting policies, processes, security controls, and procedures to mitigate identified vulnerabilities and risks.

For instance, when releasing code changes, the code is first tested in a single node, then deployed to all subsequent nodes. This process includes vulnerability checks and approval from a software engineering development lead.

MX relies on secure data center colocation facilities to house MX infrastructure including, but not limited to, data centers, physical access control, and physical security. MX uses secure colocation facilities to ensure that its data is protected from unauthorized access.

MX is passionate about and dedicated to protecting, safeguarding, and securing customer data. To do so, MX has established a strong security program supported by its Information Security team. This team runs a third-party security assessment program, where policies, controls, mechanisms, detection, and prevention are continuously improved.

Risk and Vulnerability Management

MX's Information Security team creates risk mitigation plans for each risk and is responsible for ensuring that the necessary risk alerts are sent to the MX Information Security team to review, investigate, determine root cause, and identify and execute corrective changes.

Segregation of Duties

Segregating duties in these critical processes is key to reducing the risk of fraud, unauthorized access, or other security breaches. MX systems are hardened using industry-recognized hardening standards and against external and internal threats.

Physical Security

The security of MX's physical environment is ensured by implementing security policies and controls, including authentication token management, firewalls, and physical access controls. Only authorized MX personnel can access these zones, and access is via interface tools that restrict access to these zones.

Physical Access Control and Environmental Protection

MX's Data Centers ensure secure physical access and environmental protection. All personnel check in using an electronic key card that only provides access to the zone associated with his/her job function. Visitors are escorted at all times by authorized MX personnel.

Office Buildings

MX maintains a secure physical environment across its offices, including security policies and controls that ensure that visitors check in upon arrival. Each visitor is provided with a visitor badge, which is a card that does not have the ability to enter through MX corporate office doors.

Data Centers

MX relies on secure data center colocation facilities to house MX infrastructure. These facilities are protected by firewalls, physical access controls, and logical access controls. Access to these locations does not provide logical access to systems (for logical access, see Logical Access Control).

Logical Access Control

Logical access controls ensure that only authorized personnel can access data and systems. Access to database zones containing sensitive information is limited to authorized personnel. MX relies on secure colocation facilities to house sensitive data, and access to these facilities is limited to authorized personnel.

Data Leakage Protection

MX classifies data as one of the following (listed from least to most sensitive): Public, MX Internal, and NX. Data at MX are handled commensurate with the level of data sensitivity. MX classifies data based on its sensitivity and applies access controls to ensure that only authorized personnel can access sensitive data.

Password Management

Users are authenticated to the MX production environment using strong multifactor authentication. Passwords are rotated on a quarterly basis. Authentication is performed to prevent unauthorized access to MX systems.

Audit and Compliance

MX daily operational improvements involve regularly scheduled audits and reviews. These activities help MX to continuously improve its security posture and ensure compliance with industry standards.

Incident Response

MX's Information Security team is responsible for responding to security incidents. The team is trained to respond to security incidents quickly and effectively, ensuring the timely restoration of systems and system configurations in the event of catastrophic system failure.

Summary

MX is committed to ensuring the security of its data and systems. The company deploys a defense-in-depth security model and implements a range of security controls to protect its infrastructure. MX relies on secure data centers, colocation facilities, and physical access controls to ensure the integrity of its systems and data.

MX's Information Security team is dedicated to protecting, safeguarding, and securing customer data. The team implements risk mitigation plans and continuously improves security policies and controls to ensure that MX systems remain secure.
Data Security

Data Classification, Handling, and Encryption

Data at MX are handled commensurate with the level of data sensitivity. MX classifies data as one of the following (listed from least to most sensitive): Public, MX Internal, MX Confidential, and MX Privileged and Confidential. Data classified as either MX Confidential or MX Privileged and Confidential are encrypted in transit and at rest using cryptographically strong encryption mechanisms.

For sensitive data in transit, MX encrypts transmissions using TLS 1.2. For data at rest, MX uses AES-256 keys to encrypt sensitive data.

At the end of the useful lifecycle or when requested by customers, data are destroyed securely. Media (e.g., hard disk drives) are destroyed by using Department of Defense (DoD) level drive shredding techniques.

Data Leakage Protection

Access to database zones containing sensitive information is limited to only authorized personnel. Additionally, authentication to these zones is via interface tools that restrict the extraction of sensitive data from these zones—limiting the likelihood of sensitive data leakage.
6 PERSONNEL SECURITY


**Personnel Security**

**Human Resources Security**

MX personnel are required to pass a robust background check prior to starting employment at MX. Job roles and responsibilities are communicated to MX personnel. For MX personnel with security-related roles and responsibilities, the MX Information Security team provides role-based security-related training and instruction to these personnel. MX personnel found not adhering MX Policy are subject to investigation with appropriate consequences, including disciplinary action up to termination of employment.

**Security Awareness**

MX personnel are trained and educated to be assertively security-minded. Security and compliance processes are embedded into MX’s culture, and are demonstrated by the members of MX’s organization.

As part of MX’s new hire orientation, new hires are provided a thorough information security awareness training. This training is provided as a refresher to MX personnel on an annual basis and is a requirement of employment at MX. As part of this awareness training, MX personnel are instructed to report any suspicious behavior to the MX Information Security team.
As part of MX’s new hire orientation, new hires are provided a thorough information with appropriate consequences, including disciplinary action up to termination of personnel. MX personnel found not adhering MX Policy are subject to investigation employment at MX. Job roles and responsibilities are communicated to MX personnel. MX personnel are required to pass a robust background check prior to starting.

**Personnel Security**

- Code repositories are regularly backed up to help ensure timely restore of applications.
- Likelihood of untested or potentially malicious code being deployed to production is reduced by testing the deployed code on that single node and, when confirmed successful on the node, deploying the code elsewhere.
- Code is deployed to servers in a methodical manner—deploying code to production servers one at a time.
- Configurations are pushed out to systems on an ongoing basis to help ensure systems remain hardened.
- MX systems are hardened using industry-recognized hardening standards.
- Firmware are kept up-to-date by applying the latest patches provided by network manufacturers.
- Network devices are configured to use secure configurations. Network device authentication and encryption technologies are enabled.
- Network security controls are regularly assessed by third party assessments.
- MX follows the principle of least privilege and restricts physical access to zones requiring such security.
- Logical access to MX production system components is limited to personnel having a business need and is reviewed for continued need on an ongoing basis.
- Logical access permissions and either PIN or biometric authentication are required for access to MX corporate office buildings.
- Cameras are in place to monitor for unauthorized access.
- Partitions are built with tamper-resistant hardware and extend from the building floor to the ceiling to help prevent physical intrusion.

**Data Centers**

- Customer data. To do so, MX has established a strong security program supported by internationally recognized standards (e.g., ISO 27001, NIST 800-53). MX’s Information Security team provides a mechanism for MX personnel and external users to report security-related incidents.
- MX’s Information Security team has established, maintains and executes, as needed, the MX Incident Response Plan. The plan is executed in response to a security-related incident. The plan includes procedures for how to effectively manage the incident, and restore impacted systems, see Logical Access Control. Physical access to data center colocation facilities is limited to personnel having a business need and are granted in accordance with Logical Access Control.
- Partitions are built with tamper-resistant hardware and extend from the building floor to the ceiling to help prevent physical intrusion.
- Personnel Security
- System Hardening, Baselines, and Configuration Management
- Incident Response
- Security Governance
- Third Party Vendor Risk Management
- Third Party Security
- Data Leakage Protection
- Data Security
- Assurance Reports
- Human Resources Security

**Overview**

- MX is passionate about and dedicated to protecting, safeguarding, and securing customer data. To do so, MX has established a strong security program supported by internationally recognized standards (e.g., ISO 27001, NIST 800-53).
- MX’s Information Security team provides a mechanism for MX personnel and external users to report security-related incidents.
- MX’s Information Security team has established, maintains and executes, as needed, the MX Incident Response Plan. The plan is executed in response to a security-related incident. The plan includes procedures for how to effectively manage the incident, and restore impacted systems.
- MX maintains a Business Continuity Plan that identifies business impacting systems and processes. The plan is reviewed on an ongoing basis to ensure systems and processes are supported, and tested on an annual basis.
- MX personnel. Additionally, authentication to these zones is via interface tools that restrict access permissions and either PIN or biometric authentication. Cameras are in place to monitor for unauthorized access.
- Physical access to MX corporate office buildings is secured to allow only MX personnel and external system users access. Physical access to data center colocation facilities is limited to personnel having a business need and is granted in accordance with Logical Access Control. Logical access permissions and either PIN or biometric authentication are required for access to data center colocation facilities.
- Personnel Security
- System Hardening, Baselines, and Configuration Management
- Incident Response
- Security Governance
- Third Party Vendor Risk Management
- Third Party Security
- Data Leakage Protection
- Data Security
- Assurance Reports
- Human Resources Security

**Data Centers**

- Customer data. To do so, MX has established a strong security program supported by internationally recognized standards (e.g., ISO 27001, NIST 800-53). MX’s Information Security team provides a mechanism for MX personnel and external users to report security-related incidents.
- MX’s Information Security team has established, maintains and executes, as needed, the MX Incident Response Plan. The plan is executed in response to a security-related incident. The plan includes procedures for how to effectively manage the incident, and restore impacted systems.
- Physical access to data center colocation facilities is limited to personnel having a business need and is granted in accordance with Logical Access Control. Logical access permissions and either PIN or biometric authentication are required for access to data center colocation facilities.
Third Party Security

Third Party Vendor Risk Management

MX engages with third party organizations to support MX’s ongoing operations. MX conducts a risk assessment of each third party prior to engaging with the third party. As part of this risk assessment, the services provided by a third party are evaluated to determine types of data that will be processed, facilitated, or otherwise provided to the third party. The level of sensitivity of data will determine the depth of security review performed on the third party prior to using third party services. As part of the security review, identified findings are discussed with and provided to the third party to remediate within an agreed-upon timeframe.

In addition to this initial risk assessment performed on each third party prior to engagement of services, MX conducts a review of third party security of each third party on an annual basis. Identified findings are discussed with and provided to the third party to remediate within an agreed-upon timeframe.

Assurance Reports

MX engages qualified third party assessment organizations to assess MX’s information security program (including processes described within this document) against industry-recognized security criteria and certifications. MX maintains compliance with the AICPA’s TSP, and provides evidence indicating ongoing compliance with the TSP by providing a Report on the Design and Operating Effectiveness of Controls at Service Organizations (SOC-2 Type II Report) issued by MX’s third party assessment organization.

Additionally, although MX does not intentionally process, store, or otherwise handle payment card industry (PCI) cardholder data, MX maintains compliance with applicable security requirements listed in the Payment Card Industry Data Security Standard (PCI DSS) to help ensure that any data that may fall under this provision is handled accordingly. MX provides evidence indicating ongoing compliance with PCI DSS as assessed by MX’s third party assessment organization.

Both the MX SOC-2 Type II Report and PCI DSS Attestation of Compliance are updated on an annual basis. These compliance reports can be provided to MX customers with an effective non-disclosure agreement (NDA) in place. MX customers request these reports via written request to MX’s Information Security team via email (security@mx.com).
Summary

MX invests heavily in reducing security risks at each layer of MX’s organization and each level of MX’s infrastructure. Part of MX’s security program includes a continuous improvement program, where policies, controls, mechanisms, detection and prevention systems, threats, and risks are reviewed, evaluated, and enhanced to achieve progressive hardening against external and internal threats.

Please direct any questions to security@mx.com