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:

<table>
<thead>
<tr>
<th>1</th>
<th>Security Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Strategy, Program, and Policies</td>
</tr>
<tr>
<td></td>
<td>Risk and Vulnerability Management</td>
</tr>
<tr>
<td></td>
<td>Incident Response</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>Physical Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Physical Access and Environmental Protection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>System Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Logical Access Control</td>
</tr>
<tr>
<td></td>
<td>Network Security</td>
</tr>
<tr>
<td></td>
<td>System Hardening, Baselines, and Configuration Management</td>
</tr>
<tr>
<td></td>
<td>Logging, Monitoring, and Alerting</td>
</tr>
<tr>
<td></td>
<td>Segregation of Duties</td>
</tr>
<tr>
<td></td>
<td>System Resiliency, Business Continuity, and Disaster Recovery</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>Application Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Code Security and Change Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5</th>
<th>Data Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Classification, Handling, and Encryption</td>
</tr>
<tr>
<td></td>
<td>Data Leakage Protection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6</th>
<th>Personnel Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Human Resources Security</td>
</tr>
<tr>
<td></td>
<td>Security Awareness</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7</th>
<th>Third Party Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Third Party Vendor Risk Management</td>
</tr>
<tr>
<td></td>
<td>Assurance Reports</td>
</tr>
</tbody>
</table>
Code repositories are regularly backed up to help ensure timely restore of applications and systems in the event of catastrophic system failure. Critical system data are regularly backed up to help ensure timely restoration of error, and other potential malicious activities.

MX segregates its development, Quality Assurance (QA), and production environments to maintain baseline configurations. System configuration deviations are identified, logged, and 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.

Security Strategy, Program, and Policies

MX’s security strategy is based on the principle of least privilege and the concept of defense in depth. Each layer of MX’s environment is hardened with industry-recognized standards such as the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) benchmarks.

Segregation of Duties

Segregation of duties is enforced across MX’s organization to prevent fraudulent activities. Access to sensitive information is restricted to those who need it for their job responsibilities.

Incident Response

MX has an incident response plan that is reviewed and updated on a regular basis. MX’s incident response team is responsible for identifying and executing corrective changes. MX’s Information Security team provides a mechanism for MX personnel and external parties to report security-related incidents directly to the team.

Risk and Vulnerability Management

MX conducts risk assessments and vulnerability scans on a regular basis to identify and mitigate potential security threats. MX implements risk mitigation plans and monitors their effectiveness.

Data Security

For sensitive data in transit, MX encrypts transmissions using TLS 1.2. For data at rest, MX uses industry-recognized best practices such as disk encryption and access controls.

Logging, Monitoring, and Alerting

MX’s log management system captures events from various sources such as system logs, application logs, and user activity. Monitoring systems are set up to identify deviations from baseline configurations and initiate alerts.

Physical Access and Environmental Protection

MX personnel are required to pass a robust background check prior to starting employment. Visitors are required to check in at the data center colocation facilities and are escorted at all times by authorized MX personnel. Physical access to MX’s facilities is granted to authorized individuals via electronic key cards.

Summary

MX’s security approach is based on a comprehensive suite of security, confidentiality, and privacy policies, processes, and governance. MX enacts defense in depth by hardening each layer of MX’s environment and implementing industry-recognized best practices.

Contact Support

To contact MX’s support team, visit the “Contact Support” links available in MX’s applications, or by e-mailing security@mx.com. MX’s Risk Management dashboard is communicated to MX’s management team on a periodic basis and is reviewed on a regular basis for appropriateness. The status of risk mitigation activities contained within the dashboard is communicated to MX’s management team. MX’s Information Security team is responsible for the effective implementation of information security strategy. MX enacts defense in depth by hardening each layer of MX’s environment and implementing industry-recognized best practices.

Security Awareness Training

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 these policies and procedures in their roles and responsibilities.

Personnel Security

For MX personnel with security-related roles and responsibilities, background checks are conducted to ensure that they meet the requirements for a security clearance. Personnel are required to pass a robust background check prior to starting employment.

Data Center Colocation Facilities

Data center colocation facilities are required to maintain compliance with the Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Sarbanes-Oxley Act (SOX) regulations. Physical access to the facilities is restricted to authorized personnel.

TTPs and Risk Management

MX follows the principle of least privilege and the concept of defense in depth. MX’s Information Security team provides a mechanism for MX personnel and external parties to report security-related incidents directly to the team. MX’s Risk Management dashboard is communicated to MX’s management team on a periodic basis and is reviewed on a regular basis for appropriateness. The status of risk mitigation activities contained within the dashboard is communicated to MX’s management team. MX’s Information Security team is responsible for the effective implementation of information security strategy. MX enacts defense in depth by hardening each layer of MX’s environment and implementing industry-recognized best practices.

Data Security

For sensitive data in transit, MX encrypts transmissions using TLS 1.2. For data at rest, MX uses industry-recognized best practices such as disk encryption and access controls.

Logging, Monitoring, and Alerting

MX’s log management system captures events from various sources such as system logs, application logs, and user activity. Monitoring systems are set up to identify deviations from baseline configurations and initiate alerts.

Physical Access and Environmental Protection

MX personnel are required to pass a robust background check prior to starting employment. Visitors are required to check in at the data center colocation facilities and are escorted at all times by authorized MX personnel. Physical access to MX’s facilities is granted to authorized individuals via electronic key cards.

Summary

MX’s security approach is based on a comprehensive suite of security, confidentiality, and privacy policies, processes, and governance. MX enacts defense in depth by hardening each layer of MX’s environment and implementing industry-recognized best practices.

Contact Support

To contact MX’s support team, visit the “Contact Support” links available in MX’s applications, or by e-mailing security@mx.com. MX’s Risk Management dashboard is communicated to MX’s management team on a periodic basis and is reviewed on a regular basis for appropriateness. The status of risk mitigation activities contained within the dashboard is communicated to MX’s management team. MX’s Information Security team is responsible for the effective implementation of information security strategy. MX enacts defense in depth by hardening each layer of MX’s environment and implementing industry-recognized best practices.

Security Awareness Training

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 these policies and procedures in their roles and responsibilities.

Personnel Security

For MX personnel with security-related roles and responsibilities, background checks are conducted to ensure that they meet the requirements for a security clearance. Personnel are required to pass a robust background check prior to starting employment.

Data Center Colocation Facilities

Data center colocation facilities are required to maintain compliance with the Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Sarbanes-Oxley Act (SOX) regulations. Physical access to the facilities is restricted to authorized personnel.

TTPs and Risk Management

MX follows the principle of least privilege and the concept of defense in depth. MX’s Information Security team provides a mechanism for MX personnel and external parties to report security-related incidents directly to the team. MX’s Risk Management dashboard is communicated to MX’s management team on a periodic basis and is reviewed on a regular basis for appropriateness. The status of risk mitigation activities contained within the dashboard is communicated to MX’s management team. MX’s Information Security team is responsible for the effective implementation of information security strategy. MX enacts defense in depth by hardening each layer of MX’s environment and implementing industry-recognized best practices.

Data Security

For sensitive data in transit, MX encrypts transmissions using TLS 1.2. For data at rest, MX uses industry-recognized best practices such as disk encryption and access controls.

Logging, Monitoring, and Alerting

MX’s log management system captures events from various sources such as system logs, application logs, and user activity. Monitoring systems are set up to identify deviations from baseline configurations and initiate alerts.

Physical Access and Environmental Protection

MX personnel are required to pass a robust background check prior to starting employment. Visitors are required to check in at the data center colocation facilities and are escorted at all times by authorized MX personnel. Physical access to MX’s facilities is granted to authorized individuals via electronic key cards.

Summary

MX’s security approach is based on a comprehensive suite of security, confidentiality, and privacy policies, processes, and governance. MX enacts defense in depth by hardening each layer of MX’s environment and implementing industry-recognized best practices.

Contact Support

To contact MX’s support team, visit the “Contact Support” links available in MX’s applications, or by e-mailing security@mx.com. MX’s Risk Management dashboard is communicated to MX’s management team on a periodic basis and is reviewed on a regular basis for appropriateness. The status of risk mitigation activities contained within the dashboard is communicated to MX’s management team. MX’s Information Security team is responsible for the effective implementation of information security strategy. MX enacts defense in depth by hardening each layer of MX’s environment and implementing industry-recognized best practices.

Security Awareness Training

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 these policies and procedures in their roles and responsibilities.

Personnel Security

For MX personnel with security-related roles and responsibilities, background checks are conducted to ensure that they meet the requirements for a security clearance. Personnel are required to pass a robust background check prior to starting employment.

Data Center Colocation Facilities

Data center colocation facilities are required to maintain compliance with the Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Sarbanes-Oxley Act (SOX) regulations. Physical access to the facilities is restricted to authorized personnel.

TTPs and Risk Management

MX follows the principle of least privilege and the concept of defense in depth. MX’s Information Security team provides a mechanism for MX personnel and external parties to report security-related incidents directly to the team. MX’s Risk Management dashboard is communicated to MX’s management team on a periodic basis and is reviewed on a regular basis for appropriateness. The status of risk mitigation activities contained within the dashboard is communicated to MX’s management team. MX’s Information Security team is responsible for the effective implementation of information security strategy. MX enacts defense in depth by hardening each layer of MX’s environment and implementing industry-recognized best practices.

Data Security

For sensitive data in transit, MX encrypts transmissions using TLS 1.2. For data at rest, MX uses industry-recognized best practices such as disk encryption and access controls.

Logging, Monitoring, and Alerting

MX’s log management system captures events from various sources such as system logs, application logs, and user activity. Monitoring systems are set up to identify deviations from baseline configurations and initiate alerts.

Physical Access and Environmental Protection

MX personnel are required to pass a robust background check prior to starting employment. Visitors are required to check in at the data center colocation facilities and are escorted at all times by authorized MX personnel. Physical access to MX’s facilities is granted to authorized individuals via electronic key cards.

Summary

MX’s security approach is based on a comprehensive suite of security, confidentiality, and privacy policies, processes, and governance. MX enacts defense in depth by hardening each layer of MX’s environment and implementing industry-recognized best practices.

Contact Support

To contact MX’s support team, visit the “Contact Support” links available in MX’s applications, or by e-mailing security@mx.com. MX’s Risk Management dashboard is communicated to MX’s management team on a periodic basis and is reviewed on a regular basis for appropriateness. The status of risk mitigation activities contained within the dashboard is communicated to MX’s management team. MX’s Information Security team is responsible for the effective implementation of information security strategy. MX enacts defense in depth by hardening each layer of MX’s environment and implementing industry-recognized best practices.

Security Awareness Training

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 these policies and procedures in their roles and responsibilities.
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.
Members of MX's organization. MX personnel are trained and educated to be assertively security-minded. Security and MX personnel found not adhering MX Policy are subject to investigation for employment at MX. Job roles and responsibilities are communicated to MX personnel.

Personnel Security

External penetration tests. MX conducts external penetration tests to assess the security posture of the organization. The tests are designed to simulate potential attacks and identify vulnerabilities. Third-party assessment organizations are engaged to conduct these tests. The results of the tests are reviewed by the MX Information Security team. To facilitate this process, MX's Incident Response Plan is updated and reviewed as needed.

Risk and Vulnerability Management

Risk and vulnerability management involves assessing the likelihood of sensitive information being compromised or misused. MX conducts periodic risk assessments to identify potential risks and vulnerabilities. The results of these assessments are reviewed by the Head of Security and used to create risk mitigation plans. These plans are executed by the MX Information Security team. The results of the risk assessments are reviewed by the Head of Security using the Risk Management dashboard. The dashboard consolidates information from all risk detection activities.

Security Strategy, Program, and Policies

MX's Information Security team creates risk mitigation plans for each risk. These plans are reviewed and executed by the information security team. The results of the risk mitigation plans are reviewed and updated by the Head of Security. These updates are reviewed by the Head of Security using the Risk Management dashboard. The dashboard consolidates information from all risk detection activities.

Physical Access Control and Environmental Protection

Physical access control and environmental protection involves controlling access to the physical environment. MX follows the principle of least privilege, which means that personnel are granted only the access they need to perform their job functions. 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. A badge is a card that does not have the ability to enter through MX corporate office doors. Additionally, although MX does not intentionally process, store, or otherwise handle payment card industry (PCI) cardholder data, MX maintains compliance with applicable standards. MX engages qualified third party assessment organizations to request these reports via written request to MX's Information Security team via email (security@mx.com).

MX's Disaster Recovery Plan is reviewed, updated (as needed), and tested on a periodic basis. The plan lists and describes critical system components, identifies recovery time and point objectives, and contains procedures to recover from a catastrophic system failure. The plan is executed by the MX Information Security team. The results of the plan are reviewed by the Head of Security using the Risk Management dashboard. The dashboard consolidates information from all risk detection activities.

MX equipment is isolated in secured partitions in each data center colocation facility. MX equipment is hardened using industry-recognized hardening standards such as the Center for Internet Security (CIS) benchmarks. MX systems are hardened using industry-recognized hardening standards such as the Center for Internet Security (CIS) benchmarks. MX systems are hardened using industry-recognized hardening standards such as the Center for Internet Security (CIS) benchmarks. MX systems are hardened using industry-recognized hardening standards such as the Center for Internet Security (CIS) benchmarks. MX systems are hardened using industry-recognized hardening standards such as the Center for Internet Security (CIS) benchmarks. MX systems are hardened using industry-recognized hardening standards such as the Center for Internet Security (CIS) benchmarks.

Logical Access Control

Logical access control involves controlling access to systems and system configurations using access permissions and either PIN or biometric authentication. MX uses Secure Shell (SSH) for access control. Access control is reviewed on a periodic basis for appropriateness, and physical access is removed when personnel leave MX. Access to systems and system configurations in the event of catastrophic system failure is also reviewed on a periodic basis. As noted above, OS baselines and associated system configurations, code repositories, and patches are applied to systems. The MX Information Security team has defined critical security alert criteria. These criteria are used to determine the likelihood of sensitive information being compromised or misused. The criteria are reviewed on a periodic basis. For sensitive data in transit, MX encrypts transmissions using TLS 1.2. For data at rest, MX maintains compliance with ISO 27001 Data Protection. Confidential or MX Privileged and Confidential are encrypted in transit and at rest using AICPA's assurance reports.
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.
compliance processes are embedded into MX's culture, and are demonstrated by the employment. 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 from subfloor to system users to report potential security incidents. MX personnel are encouraged and needed), and tested on an annual basis. MX's Information Security team provides a mechanism for MX personnel and external visitors to MX corporate office buildings check in at the reception desk. Each visitor’s 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. Visitors to MX corporate office buildings are escorted at all times by authorized MX personnel.

MX invests heavily in reducing security risks at each layer of security governance, security strategy, program, and policies, system hardening, baselines, and configuration management, risk and vulnerability management, application security, segregation of duties, physical access to MX corporate office buildings is secured to allow only MX personnel to enter. MX personnel terminate their employment for any reason. MX's approach to security includes a defense-in-depth strategy. This strategy is designed to protect against a wide range of potential threats, including those that are novel and unknown.

MX's Risk Management dashboard are communicated to MX's management team on a regular basis—accounting for updates and changes to the dashboard. Risk and vulnerability management is an ongoing process that involves identifying, assessing, and mitigating potential threats to the organization’s systems and data.

MX deploys a defense-in-depth strategy, which means that security measures are layered and redundant, helping to prevent unauthorized access to systems and data. MX's approach to security includes a defense-in-depth strategy. This strategy is designed to protect against a wide range of potential threats, including those that are novel and unknown.

MX's approach to security includes a defense-in-depth strategy. This strategy is designed to protect against a wide range of potential threats, including those that are novel and unknown. MX deploys a defense-in-depth security model—securing MX systems from subfloor to system users to report potential security incidents. MX personnel are encouraged and needed), and tested on an annual basis. MX's Information Security team provides a mechanism for MX personnel and external visitors to MX corporate office buildings check in at the reception desk. Each visitor’s 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. Visitors to MX corporate office buildings are escorted at all times by authorized MX personnel.

MX invests heavily in reducing security risks at each layer of security governance, security strategy, program, and policies, system hardening, baselines, and configuration management, risk and vulnerability management, application security, segregation of duties, physical access to MX corporate office buildings is secured to allow only MX personnel to enter. MX personnel terminate their employment for any reason. MX's approach to security includes a defense-in-depth strategy. This strategy is designed to protect against a wide range of potential threats, including those that are novel and unknown.

MX deploys a defense-in-depth strategy, which means that security measures are layered and redundant, helping to prevent unauthorized access to systems and data. MX's approach to security includes a defense-in-depth strategy. This strategy is designed to protect against a wide range of potential threats, including those that are novel and unknown.

MX's Risk Management dashboard are communicated to MX's management team on a regular basis—accounting for updates and changes to the dashboard. Risk and vulnerability management is an ongoing process that involves identifying, assessing, and mitigating potential threats to the organization’s systems and data.

MX deploys a defense-in-depth strategy, which means that security measures are layered and redundant, helping to prevent unauthorized access to systems and data. MX's approach to security includes a defense-in-depth strategy. This strategy is designed to protect against a wide range of potential threats, including those that are novel and unknown.

MX's Risk Management dashboard are communicated to MX's management team on a regular basis—accounting for updates and changes to the dashboard. Risk and vulnerability management is an ongoing process that involves identifying, assessing, and mitigating potential threats to the organization’s systems and data. MX uses AES-256 keys to encrypt sensitive data. The MX Incident Response Plan should be executed, procedures for how to effectively faciliate 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 Risk Management dashboard are communicated to MX's management team on a regular basis—accounting for updates and changes to the dashboard. Risk and vulnerability management is an ongoing process that involves identifying, assessing, and mitigating potential threats to the organization’s systems and data. MX uses AES-256 keys to encrypt sensitive data. 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.
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 perform 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.
How MX Protects 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 Human Resources Security external penetration tests.

vulnerability and risk detection mechanisms including, but not limited to, continuous MX deploys a defense-in-depth security model—securing MX syste

MX's approach to security includes a defense-in-depth strategy. This strategy is

access to only a select set of individuals with the ability to deploy code reduces the

Code deployment is limited to only authorized software developm

Code is deployed to servers in a methodical manner—deploying co

change, a peer review, systematic code style checks, code security review (including

Application code is managed and deployed using a centrally managed software

firmware are kept up-to-date by applying the latest patches pro

privilege by provisioning only the needed permissions to users in order to perform

Logical access to MX production system components is limited to

Visitors are escorted at all times by authorized MX personnel.

identity is authenticated using a government-issued identification. Visitors are required to

MX personnel are required to wear their MX identification (or I.D.) badge in a manner

Physical access to MX corporate office buildings is secured to allow only MX personnel

Partitions are built with tamper-resistant hardware and extend

MX equipment is isolated in secured partitions in each data center colocation facility.

Physical Security

a comprehensive suite of security, confidentiality, and privacy policies, processes,

Overview

data leakage.

For sensitive data in transit, MX encrypts transmissions using TLS 1.2. For data at rest,
cryptographically strong encryption mechanisms.

Data at MX are handled commensurate with the level of data sensitivity. MX classifies

system users to report potential security incidents. MX personnel are encouraged and

the MX Incident Response Plan should be executed, procedures for how to effectively

MX's Risk Management dashboard are communicated to MX's management team on a

executes these risk mitigation plans. Status of risk mitigation activities contained within

Results of these risk detection activities are consolidated and

MX maintains a Business Continuity Plan that identifies business impacting systems and

As noted above, OS baselines and associated system configurations, code repositories,

Segregation of Duties

Logical Access Control

Incident Response

Security Strategy, Program, and Policies

Security Governance

Segregation of Duties

Logical Access Control

Incident Response

Security Strategy, Program, and Policies

Security Governance

4

APPLICATION SECURITY
**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.
MX personnel are trained and educated to be assertively secure. MX personnel found not adhering MX Policy are subject to investigation.

Human Resources Security

MX deploys a defense-in-depth security model—securing MX systems at each level and layer. To proactively identify potential risks, MX deploys several security strategies. MX enacts defense in depth by hardening each layer of MX's systems, supporting policies, processes, security controls, and procedures.

Security Governance

MX's incident response and root cause analysis processes. Logs are in read-only format and are accessed only by authorized personnel. Logs are sufficiently detailed to support investigation of security events.

System, database, and application activities are logged and monitored for irregular and unusual activity.

MX invests heavily in reducing security risks at each layer of its organization and each system level.

Data Security

Confidential or MX Privileged and Confidential data is encrypted in transit and at rest using industry-standard cryptography.

Data Classification, Handling, and Encryption

External system users are able to report security-related incidents to the MX Security Operations Center (MX SOC).

MX's Information Security team has established, maintains, and executes, as needed, procedures, critical dependencies, and strategy plans to restore business operations in the event of catastrophic system failure.

MX's incident response and root cause analysis processes.

MX's incident response and root cause analysis processes.

MX's incident response and root cause analysis processes.

MX's incident response and root cause analysis processes.

MX invests heavily in reducing security risks at each layer of its organization and each system level.

MX invests heavily in reducing security risks at each layer of its organization and each system level.

MX invests heavily in reducing security risks at each layer of its organization and each system level.
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.
How MX Protects

Awareness training, MX personnel are instructed to report any suspicious behavior to Human Resources Security on an annual basis and is a requirement of employment at MX. As part of this, MX personnel are trained and educated to be assertively security-conscious.

As part of MX’s new hire orientation, new hires are provided a thorough information security strategy. MX enacts defense in depth by hardening each layer of MX’s systems, threats, and risks are reviewed, evaluated, and enhanced to achieve progressive improvement program, where policies, controls, mechanisms, detection and prevention include a defense-in-depth strategy. This strategy is supported by policies, processes, security controls, and procedures, and security controls. This security whitepaper highlights MX’s security governance, personnel security, and physical security.

MX’s approach to security includes a defense-in-depth strategy. This strategy is supported by policies, processes, security controls, and procedures. This security whitepaper highlights MX’s security governance, personnel security, and physical security.

MX personnel with security-related roles and responsibilities are trained and educated to be assertively security-conscious. MX personnel are instructed to report any suspicious behavior to Human Resources Security on an annual basis and is a requirement of employment at MX. As part of this, MX personnel are trained and educated to be assertively security-conscious.

For MX personnel with security-related roles and responsibilities, the MX Information Security Program ensures that all policies, processes, and procedures are reviewed and approved on a periodic basis. Any blockers identified in risk mitigation activities are provided to MX’s Risk Management dashboard. The MX Risk Management dashboard is reviewed by the Head of Information Security on a periodic basis. Any blockers identified in risk mitigation activities are provided to MX’s Risk Management dashboard. The MX Risk Management dashboard is reviewed by the Head of Information Security on a periodic basis.

MX’s Information Security Program includes a continuous vulnerability and risk detection mechanisms including, but not limited to, continuous monitoring, access control, and threat hunting. MX’s Information Security Program also includes a defense-in-depth strategy. This strategy is supported by policies, processes, security controls, and procedures. This security whitepaper highlights MX’s security governance, personnel security, and physical security.

MX personnel terminate their employment for any reason. In order to support MX’s Business Continuity Plan, MX has a Disaster Recovery Plan that includes procedures for how to effectively recover from a disaster. The MX Disaster Recovery Plan is reviewed on a periodic basis. Any blockers identified in risk mitigation activities are provided to MX’s Risk Management dashboard. The MX Risk Management dashboard is reviewed by the Head of Information Security on a periodic basis. Any blockers identified in risk mitigation activities are provided to MX’s Risk Management dashboard. The MX Risk Management dashboard is reviewed by the Head of Information Security on a periodic basis.
How MX Protects Your Data

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.
7
THIRD PARTY SECURITY

security awareness training. This training is provided as a refresher to MX personnel as part of MX’s new hire orientation, new hires are provided a thorough information security briefing. As part of MX’s organization, members of MX’s organization are provided with appropriate training, including compliance processes that are embedded into MX’s culture, and are demonstrated by the Personnel Security Team.

MX’s approach to security includes a defense-in-depth strategy. This strategy is designed to protect against a wide range of threats, including both external and internal attacks. The strategy is comprised of several key components, including:

- **Security Governance:**
  - MX’s governing body is responsible for setting the overall security strategy and ensuring that it aligns with business needs.
  - MX’s Board of Directors is responsible for overseeing the company’s overall security strategy and ensuring compliance with relevant laws and regulations.

- **Risk and Vulnerability Management:**
  - MX is committed to managing the risk associated with its business operations and the protection of its sensitive data.
  - MX conducts regular risk assessments and vulnerability scans to identify potential threats.

- **Data Center Security:**
  - MX relies on secure data center colocation facilities to house its infrastructure, including critical systems and data.
  - MX is committed to maintaining compliance with relevant laws and regulations, including the Payment Card Industry Data Security Standard (PCI DSS).

- **Logical Access Control:**
  - MX employs strict access controls to ensure that only authorized personnel have access to critical systems and data.
  - Access control is enforced through a combination of physical and logical mechanisms.

- **Application Security:**
  - MX is committed to ensuring the security of its applications.
  - MX employs a variety of techniques to detect and prevent security vulnerabilities, including code reviews and vulnerability assessments.

- **Code Security and Change Management:**
  - MX is committed to ensuring that its software is secure and free from vulnerabilities.
  - MX employs a variety of techniques to detect and prevent security vulnerabilities, including code reviews and vulnerability assessments.

- **System Hardening, Baselines, and Configuration Management:**
  - MX is committed to ensuring that its systems are configured to meet security standards.
  - MX employs a variety of techniques to detect and prevent security vulnerabilities, including code reviews and vulnerability assessments.

MX’s incident response plan is designed to respond to security incidents in a timely and effective manner. The plan includes a variety of procedures, including:

- **Detection and Response:**
  - MX employs a variety of monitoring and alerting systems to detect security incidents.
  - MX’s incident response team is notified immediately upon detection of a security incident.

- **Containment and Mitigation:**
  - MX employs a variety of techniques to contain and mitigate the impact of security incidents.
  - MX’s incident response team is responsible for implementing containment and mitigation strategies.

- **Recovery and Post-Mortem:**
  - MX employs a variety of techniques to recover from security incidents.
  - MX’s incident response team is responsible for conducting a post-incident review to identify lessons learned and improve the incident response plan.

MX is committed to maintaining the security of its data and systems, and is dedicated to continuously improving its security practices and processes.
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 additional 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