AAA-ICDR® Information Security Program

The security and privacy of customer and case information is a top priority for the American Arbitration Association-International Centre for Dispute Resolution® (the "AAA-ICDR"). The AAA-ICDR has implemented best practice policies, procedures and technologies to help protect its data and information systems. The protections we have implemented apply to all case data and equipment stored and managed on the AAA-ICDR's technology infrastructure. With increased concerns about information security, the AAA-ICDR continues to invest significant resources and staff to maintain the highest caliber of data protection.

Organizational Support and Oversight

The AAA-ICDR maintains a formal Information Security Program with senior management level governance. The AAA-ICDR's Information Security Committee (ISC), comprised of senior staff from IS, HR, Legal and the business, provides comprehensive oversight of the systems and processes employed to protect the AAA-ICDR's information assets and electronic systems. The ISC is responsible for setting information security policies, driving security awareness, evaluating new threats and reducing risk of intrusion, loss of data integrity and compliance violations. It evaluates and sets acceptable levels of risk, coordinates organization wide information security initiatives, suggests and evaluates resources for addressing information security concerns, and generates new initiatives as needed to improve AAA-ICDR's information security posture.

ISC members are also expected to act as custodians of the enterprise security program by ensuring visible executive support, as well as communicating progress and achievements. The role of a permanent governance structure, not only ensures high quality program outcomes, but all also reinforces the message that enterprise security is an ongoing, long-term initiative.

Ensuring Program Effectiveness

To ensure the effectiveness of the AAA-ICDR's Information Security Program, the AAA-ICDR undertakes several information security related assessments, audits and security tests annually.

The AAA-ICDR formally scores all its security controls against the National Institute of Standards and Technology (NIST) Cybersecurity Framework providing a quantitative view of risks, ensuring alignment with industry standards and providing specific and actionable control/mitigation recommendations.

The AAA-ICDR also conducts Information Security Risk Assessment workshops annually with input and participation from business units across all major divisions and locations to determine areas of potential vulnerability related to the AAA-ICDR's data, systems and infrastructure, and to initiate appropriate remediation as needed.

In addition to these assessments, the AAA-ICDR systems and controls are examined and validated as part of several formal annual audits and security tests. The audits include a formal IT General Controls Audits performed by CohnReznik,

the AAA-ICDR's financial auditors, as well as Security Configuration Audits conducted by our software and vendor partners to ensure that the AAA-ICDR's network and systems are properly configured to minimize threats and optimize performance.

The AAA-ICDR also engages a third party security firm to conduct both an external and internal penetration test as well as social engineering tests to ensure staff compliance with the AAA-ICDR's confidentiality polices.

All findings or recommendations resulting from any of the AAA-ICDR's security assessments, audits or tests are tracked by the ISC to ensure timely remediation.

Key Protections

The AAA-ICDR employs several layers of advanced and best practice protections against both external and internal cyber threats. These protections include the following:

- AAA-ICDR data and systems are housed in off-site secure access data centers that comply with the security regulations set up by the American Institute of Certified Public Accountants (AICPA) for Service Organization Control (SOC) type II reports.
- The AAA-ICDR utilizes industry standard next generation firewalls (communication management computers specially designed to keep information secure and inaccessible by unauthorized Internet users), antivirus and other related security technologies to secure our network and websites. Internet of Things (IoT) devices (e.g. security cameras, card key entry systems, etc.) are configured to run in a separate and segmented network.
- Security patches are applied regularly to all AAA-ICDR systems following a formal Patch Management Policy.
- Advanced Security Information and Event Management (SIEM) software products and services are in place to monitor internal networks for suspicious user activity and to alert appropriate staff as needed.
- Unique usernames and passwords are required to access AAA-ICDR systems. Users only see what they have been given permission to see given their role within the organization.
- The AAA-ICDR employs extensive use of advanced (AES 256-bit TLS) encryption (the scrambling of sensitive data) across it's hardware and systems including:
    - All data stored in either of the AAA-ICDR datacenters completely encrypted at storage level; case record data in software and development and test environments anonymized.
    - The AAA-ICDR encrypts all data sent over the internet and ensures it is unreadable if intercepted.
    - All AAA-ICDR employee laptops are protected with full disk encryption, which prevents unauthorized access to any data on the laptop in the event it is stolen or lost.
    - AAA-ICDR systems require removable media (e.g. pen drives) to be encrypted.
- Customers wishing to pay invoices by credit card must process their own payments directly online. AAA-ICDR payment pages are configured to facilitate the entry of credit card data directly into the site of a third party, industry leading credit card processing company who is Payment Card Industry Data Security Standard (PCI DSS) compliant. No credit card information is ever transmitted or stored on AAA-ICDR systems.

- The AAA-ICDR utilizes Mobile Device Management to enforce the use of passwords or pins on personal devices used to view AAA-ICDR email and can remotely remove all AAA-ICDR email from a device reported as lost or stolen.
- Data regularly auto purged to ensure compliance with data retention policies.

Incident Response and Recovery

The AAA-ICDR has in place both a formal Cyber Security Incident Response Plan as well as a Disaster Recovery Plan (DRP) to address both the management and potential recovery from a cyber attack.

Aside from the IS team's monitoring of AAA-ICDR's technology systems, all AAA-ICDR employees and authorized users of the AAA-ICDR's information assets have been trained and are required to report any violations of the Acceptable Use Policy and/or any potential Incident to the IS team.

The Cyber Security Incident Response Plan describes the overall plan for responding to information security incidents. The goal of the Incident Response Plan is to detect and react to cyber security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

The AAA-ICDR Security Incident Response Team is comprised of system and network administrators, technical support staff, the AAA-ICDR's Chief Information Officer (CIO), computer security program managers, legal representation and others responsible for preparing for or responding to cyber security incidents at the AAA-ICDR. The Plan defines the roles and responsibilities of these participants throughout the incident response process.

In the event of a technology outage or systems damage caused by a cyberattack, the AAA-ICDR will employ its Disaster Recovery Plan (see Business Continuity and Disaster Recovery section for full summary of the DRP).

The AAA-ICDR maintains two, highly resilient, data centers, a primary data center located in Secaucus, NJ and a secondary data center located in Plano, TX. Both data centers house a copy of system images and data which is synchronized in real time. The secondary data center can be used in conjunction with, or in the case of a disaster, as a replacement to the primary data center. We also run daily backups of all production data which are stored securely both on and off site. Both data centers employ a high-level of server virtualization, clustering and equipment redundancy, thus allowing for real-time failover of key business applications and/or connectivity in the event of an equipment failure.

Security Awareness

Quarterly Security Awareness themes are established and communicated to all staff. Theme subject matter is reinforced through required monthly on-line trainings, physical posters placed in all AAA-ICDR offices, and Security Alerts sent via email. In addition, all AAA-ICDR staff must complete at least two hours of information security-related trainings annually.

Staff are also required to annually acknowledge and sign an Acceptable Use Policy which outlines the appropriate and secure use of the AAA-ICDR's resources and data.

Lastly, given that the majority of system breaches are initiated via a Phishing attack, the AAA-ICDR has invested heavily in training all staff on how to identify a Phishing attack and how to avoid being caught by one. The AAA-ICDR also preforms regular mock phishing tests and has a disciplinary process in place for staff that fail the tests repeatedly.