# We Work Hard to Keep Your Data Safe.

*Andera's Information Security Program protects your information assets with a seven point program.*

## Our Mission

Andera's Information Security Program mission is: "To provide for the security of corporate information assets, while enabling Andera to meet corporate goals in an environment where information is available to those who need it, and is protected from unauthorized disclosure, alteration, misuse, and destruction."

## Our Team

Andera has a dedicated security team that, following best practices, remains independent from the development, implementation, and sale of our products. Our security team is responsible for enforcing our Information Security Program and educating the company on security threats.

## Seven Point Program

Seven broad policies form the framework for Corporate information security's risk-based program:

| Policy | Description | Standards |
|---|---|---|
| Information Classification | Andera defines, identifies, classifies, and labels its information assets based on criticality, sensitivity, and integrity. All sensitive, company confidential, corporate generated and/or managed data must be so labeled. | • Data identification<br>• Data classification<br>• Data labeling |
| Asset Protection | Andera protects the confidentiality, integrity, and availability of all information assets under its care. Access controls (including remote access, remote control, and/or physical access), granted on a “need-to-know” basis, are required for all protected public and company confidential information. | • Remote access & control restrictions<br>• Physical access restrictions<br>• Encryption<br>• Network security<br>• Availability protection<br>• Integrity Protection<br>• Handling of Information<br>• Auditing and logging<br>• Patch management<br>• Data retention<br>• Virus Protection<br>• Insurance |
| Asset Management | Andera requires prudent management of its technology infrastructure, including networks, systems, applications, and processes throughout their respective life cycles. This management approach ensures a securely designed, implemented, and maintained asset protection environment. | • Life cycle management<br>• Configuration management<br>• Change management<br>• Systems development life cycle management |
| Acceptable Use | Andera requires the appropriate business use of all information assets under its care. This includes, but is not limited to, the proper use of information systems, telecommunications systems, the Internet/intranets/extranets connections, electronic mail, voice mail, telephones, pagers, and faxes. Andera maintains the right to monitor, record, and audit the use of such systems and/or equipment, and address the reporting of potential misuse. | • Corporate code of privacy &conduct<br>• Email & internet use<br>• Computer & work area<br>• Password Use<br>• Sensitive information & proprietary information transmission protection<br>• Media disposal and re-use<br>• Security violation reporting<br>• Violation of Acceptable Use<br>• Physical access restrictions<br>• Mobile / Bring Your Own Device<br>• Information Classification and Labeling |
| Vulnerability and Risk Management | Andera continually identifies and prioritizes technical, organizational, procedural, and/or physical security weaknesses, manages the mitigation of identified risks, and maintains metrics on progress. | • Risk assessments<br>• Risk management<br>• Independent Audits<br>• On-going Internal Management Assessments<br>• Independent Security Reviews<br>• Information Security Expertise |

| | | |
|---|---|---|
| Threat and Assessment Monitoring | Andera identifies and prioritizes categories of threats and/or specific threats and seeks to deter them. Andera also employs threat detection monitoring tools to provide timely response and recovery in the event of a security breach. | • Threat assessment, detection & monitoring<br>• Disclosure & incident response |
| Security Awareness and Education | Andera requires policy framework elements and standards content be properly communicated and accessible to new hires, employees, and third parties through the provision of appropriate education and training. | • Security awareness education for new hires and security awareness availability<br>• Contracts<br>• Security Awareness and Availability |

## Security Best Practices

Andera follows industry best practice guidelines in the design and implementation of our network environment. These are just a few of our controls that adhere to security best practices:

- Multi-factor Authentication
- Intrusion prevention system
- Data and Transmission Encryption
- Security Incident and Event Management
- Network Segregation
- Anti-virus Management
- Patch Management

## Compliance Program

To ensure that Andera consistently meet all regulatory requirements, the following audits and assessments are performed regularly:

| Regulation | Frequency |
|---|---|
| Payment Card Industry (PCI) Scan | Quarterly |
| FFIEC | Biennially |
| NACHA | Annually |
| SSAE 16 | Annually |
| Internal and External Security Assessments | Annually |