**Code of Ethics**

It is the responsibility of every member of Aeries Infotech, Inc. to act in a manner that is consistent with this Code of Ethics statement and its supporting guidelines. Each staff member shall abide by this Code, as a condition of employment. No employee may allow personal preferences, convenience or business pressures to compromise this Code of Ethics. All employees have an obligation to report activities, which they believe, may be in violation of this Code of Ethics.

In an effort to deliver high-quality consulting services in a responsible and reliable manner all employees should hereby:

- Provide high-quality services
- Fairly and accurately represent this company
- Provide services to meet the needs of customers
- Adhere to appropriate standards throughout the organization
- Be honest, trustworthy and reliable in all relationships
- Pursue fiscal responsibility and growth
- Treat employees fairly
- Utilize company technology in an appropriate way (internally & externally)—maintaining confidentiality and not compromising data integrity
  1) Guideline: Prevention & control of computer abuse
  2) Guideline: Computer & network usage
  3) Guideline: Internet content & communication
  4) Guideline: Prevention & protection from viruses and other malware
  5) Guideline: Usage of licensed software, shareware, and software piracy
  6) Guideline: Workplace privacy and monitoring
  7) Guideline: Professional responsibilities—Identifying & resolving ethical IT issues

1) **Guideline: Prevention and Control of Computer Abuse**

**Definitions:**

**Information systems:** A set of information sources connected under the same control and shares functionality. It usually consists of hardware, software, data, applications, and information technology staff communications.

1. Any computer problems should be reported to information systems.
2. Any computer removal or relocation should be reported to information systems.
3. No business information should be stored on portable media unless authorized by the department supervisor. All sensitive business information should be stored on...
the Aeries Infotech shared drive to be included in routine scheduled system back-ups.

4. Personalized user IDs and passwords must be used in order to access the Aeries Infotech information system.

5. Organization-wide software patches, updates, and distributions should not be hindered in any way.

6. The corporate network will be protected by a firewall to limit inappropriate access by external computer users.

7. Data transmissions will be processed through 128-bit encryption.

8. RSID devices will be provided to employees with a loginID to access the network externally.

9. Employees must lock their computers when they leave their workstation to protect business data.

10. Employees must log off or shut down their computer when departing their shift.

11. If computer workstations are located in an unsecured area (public area), and inactivity timer must be utilized to lock the computer workstation after 5 minutes of inactivity.

12. Workstations will prompt users to change his/her password every 90 days.

13. Anti-virus software will be routinely updated on all Aeries Infotech workstations.

14. All e-mails containing executable files will be automatically blocked. To unblock these files, your supervisor will need to communicate authorization through our information systems department.

15. Employees are to guard their passwords and help protect against unauthorized access to Aeries Infotech data. If an employee is proven to be a malicious insider and co-conspirator in a data breach, he will be prosecuted to the highest level of the law and his employment will be immediately terminated.

16. It is the responsibility of every employee to report any unusual computer activity to the information systems department.

If an employee fails to abide by this guideline he will be subject to disciplinary action in accordance to Human Resources policies.
2) Guideline: Computer and Network Usage

Aeries Infotech employees shall make reasonable efforts to protect computer data, by adhering to this computer workstation guideline.

Definitions:

Computer workstation: Any computer device used to access Aeries Infotech, Inc. data

1. All hardware/software must be approved and purchased through Aeries Infotech.

2. All hardware/software must be installed by Aeries Infotech information systems staff.

3. Workstations must not be used for any activity that is in violation of Aeries Infotech guidelines, or more importantly local, state, federal, or international law.

4. Employee access to certain websites based on content such as sex, violence, and other sites that go against Aeries Infotech’s Ethics guideline will be blocked and recorded for and information & security audit. Such security audits will be conducted on a routine basis and reported to the company’s executives.

5. Workstations are property of Aeries Infotech and must be used for business operations.

6. All data stored on the workstations are property of Aeries Infotech.

7. Workstations may be monitored by information systems or security personnel.

8. If using a mobile device (i.e., smart phone) to access the Aeries Infotech network, business will need to be conducted through a virtual private network (VPN) to gain access to the corporate intranet.

3) Prevention & protection from viruses and other malware

Ethical uses of the Internet include the following:

- Using resources for business and informational purposes only, not for unauthorized, illegal or unethical purposes
- Respecting the privacy of others by not misrepresenting oneself as another user, and by not attempting to gain access to files, passwords, or data belonging to others
- Not damaging or altering software components of any network
- Bringing programs from a remote computer's hard drive to a company computer's hard drive is not permissible
- Not sending, receiving, or displaying, text or graphics which may be construed as obscene, sexually explicit, or demeaning to any race, ethnic background, religion, disability, gender, or lifestyle.

Aeries Infotech, Inc. will use a single anti-virus product for anti-virus protection. The minimum requirements shall be:

- The product shall be configured in real time on all servers and client computers.
- The library definitions shall be updated at least once daily.
- All user controlled workstations and servers shall have anti-virus scans a minimum of once per week.

Only domain administrators will be enabled to stop anti-virus definition updates and anti-virus scans.

Any e-mails with malware will be prevented from entering the network.

The e-mail server or proxy server will also be enabled to scan all email for viruses and/or malware. All email will be scanned as it enters and leaves the server. All stored email will also be scanned once weekly for viruses or malware.

When an email breaks the rules and contains an illegal file attachment:

1. Delete the email and do not notify the sender or the recipient. Training by letting users know what files are blocked can help remedy this problem.
2. Delete the email and notify the sender - This will notify senders when their emails do not go through, but it will also notify senders that they sent an email with an illegal attachment.

To increase mail security, we will add an anti-spam or proxy mail server to our network. An anti-spam server will reduce the load on the e-mail server.

When members of the public or employees of the organization send files into the network:

1. All legitimate methods to be used include:
   1. FTP transfer to a FTP server
   2. File transfer to a Web server with a legitimate file upload program
2. Files will be scanned for hostile content before they are completely transferred into the network.

All systems will be protected by a firewall any time they are connected to the internet. Computers operating outside the organizational network must have a local firewall operational at all times when connected to the company’s internet. Information Systems will specify acceptable firewall products. Mobile computers must be checked for malware before connecting to the main network.
4) Guideline: Usage of licensed software, shareware, and software piracy

Licensed Software

- New software must be approved by the IT supervisor of Aeries Info Tech. New software is to be shipped to the Information Technology department who will retain software, licenses and manuals, excluding end-user manuals.
- Installations will be performed by Aeries Info Tech IT staff. Software will not be installed without a proper license.

Shareware

- All licenses must be stored centrally within the Information Technology (IT) department. IT will maintain a license inventory of all restricted licenses to include all purchased, granted, “free” for educational use, shareware, or any other restricted license.

Piracy

The rights of software manufacturers must be strictly upheld at Aeries Info Tech, Inc. We prohibit illegal copying of copyrighted software by Aeries Info Tech employees.

- Rights of software manufacturers are protected by federal and state laws, Aeries Info Tech prohibits the engagement of illegal software copying on our property using our equipment or software.
- Each supervisor must insure that all software being used within his department has been acquired appropriately and that no illegal copies are being used outside the software program’s copyright provisions.
- An infringement of software copyrights using Aeries Info Tech equipment, will be a violation of our policy and the employee will be subject to disciplinary action. Any action initiated by the software manufacturer will be the sole responsibility of the employee.
- Each supervisor must inform his employees about our position against illegally copying copyrighted programs.

5) Guideline: Workplace Privacy & Monitoring

Privacy

- Personnel records will not be disclosed to third parties without an employee's permission.
- Employees have the right to request access to their personnel files with proper notice.
- The use of all or part of an employee’s social security number as computer passwords or employee ID numbers is prohibited.
- Social security numbers will be used on wage statements for tax purposes.
- If there is a suspected compromise to an employee’s personal information, we will disclose this fact.
- Drug testing is a requirement for new hires and the results will be kept confidential. Periodic drug testing may be required without advance notice.
- Confidential background checks are part of the hiring process.

6) Monitoring
- Telephone conversations will not be recorded without the consent of both parties being recorded.
- If the situation complies with Federal and State guidelines, we may monitor, save, record, access, use of company electronic communication resources and systems.
- Access and use of any data contained in any company-owned or -provided electronic system or tool (i.e., e-mail, Internet, and voicemail) belongs to the company, and is subject to various types of monitoring.

7) Professional Ethical Responsibilities with Information Technology (IT)
- IT professionals who develop systems must make others aware of, any potential damage to the environment.
- IT professionals must be honest and not make false claims about an IT system, but will provide disclosure of all limitations and problems.
- IT professionals are obligated to report any signs of system dangers that might result in serious damage. It may be necessary to "blow the whistle" if superiors do not help correct the problem or reduce risk.
- IT professionals must not violate copyrights, patents, trade secrets and the terms of license agreements.
- IT professionals must maintain the privacy and integrity of data. Precautions must be taken to ensure the accuracy of data, prevent unauthorized access or accidental disclosure of data.
• IT professionals must practice tolerance and respect for others. Discrimination will not be tolerated.