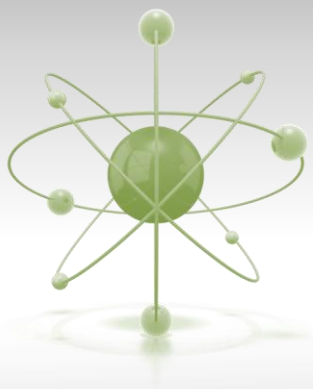
SAL System Security

The following addresses ECSI's Policies and Procedures for Security, Data Integrity, and Theft Prevention within the ECSI Data Center. ECSI's Computer Facilities operate exclusively on networked, personal computer data processing equipment. All processing is performed in-house. ECSI's data processing department includes a full-time staff of operators, programmers and systems analysts.

Information Security:
Security is a top-priority at ECSI. We provide a set of encryption routines to each client. Data is encrypted prior to exposing it to the Internet. Data is only decrypted after retrieval from the Internet servers. When sending secure information, we strongly recommend that all clients use Secure FTP to exchange data with ECSI. In addition to using Secure FTP, we also recommend that you encrypt all data prior to the exchange. All connections to ECSI are through the Internet. Secure connections for VNC are provided via Zebedee or Cisco IPSec VPN. Data to be transmitted between clients and ECSI is encrypted using software provided by ECSI utilizing 448-bit Encryption. Microsoft Terminal Server is configured for per-session, 128-bit, Bi-Directional Encryption. Web Security is provided through a 128-bit SSL connection. Data exposed to the Internet through our Web Services is Encrypted using 256-bit or 448-bit (blowfish) depending on the sensitivity of the data.
Furthermore, CCM/MSA (a Pittsburgh based Corporation) provides all second-level support for Hardware and Software Requirements. They are a Microsoft Certified Partner and all CCM/MSA Engineers assigned to the ECSI Account hold MCSE Status in all the relevant products. A PCI authorized company performs quarterly security scans of all of our internet exposed servers.



Physical Security:
All ECSI entrances are controlled via a key-lock system. A limited number of authorized personnel have physical keys to enter the facility. During normal business hours, other employees (without keys), vendors, and visitors enter the building via an intercom system.
The building is secured by an alarm system. Throughout the facility, there are fire suppression and environmental control mechanisms in place. Each floor in the building has hand-held fire extinguishers; smoke alarms, heat detectors, fire alarms, and air conditioning units. The building is also equipped with a fire suppression sprinkler system. Our computer room is temperature controlled by two separate independent air conditioning units.

Logical Security:
The SAL System may be locked down to the Field and/or Function Level. Therefore, SAL-User Access is controlled through the use of SAL User ID #s and Passwords. All SAL-Users will be setup on the network in groups based on their Job Description, Functions and/or Responsibilities. Requests to set up new SAL-Users can be done on the ECSI website, via our new Secure Forms Application. Please note: A SAL System Administrator at the University has unlimited access to Add, Change, and/or Delete SAL System Access and Rights.

Please feel free to contact us at 1-800-437-6931 or email us at clientsupport@ecsi.net and we'd be glad to assist you.