



Security is serious business and NetEnrich provides a robust framework to ensure a 100% secure service delivery for its customers.

Intrinsic elements of this framework are:

Secure NOC: NetEnrich NOCs are designed to protect customer's data from unauthorized removal. All the workstations within our NOCs are diskless and all external communication ports (except the Ethernet port) are disabled. All communications over the network are SSL encrypted.

Process: All our processes are ITIL based and documented. ITIL represents the industry's recognized best practice IT processes. Our processes have been carefully developed and tailored over time based on experience with hundreds of customers and thousands of devices to ensure the integrity and security of the customer's data and infrastructure.

Session Recordings: Each time a NetEnrich NOC engineer connects to a customer environment a recording is created that captures the entire session and can be played back later by the customer to audit the entire session, including every key stroke and each mouse click.

Certifications: NetEnrich is ISO 27001 certified. ISO 27001 formally specifies a management system that brings information security under explicit management control. This mandates specific requirements including formal audits that ensure certified compliance with the standard.

Our specification:

- Systematically examines the organization's information security risks, taking account of the threats, vulnerabilities and impacts.
- Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that it deems unacceptable.
- Adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

SAS70: The NetEnrich environment is SAS70 audited for adherence to all of our defined processes. This provides the customer with the final assurance that NetEnrich not only has well defined processes, but that we also document and follow those processes.

Secure Data Centers: Our data center is hosted with world class amenities which include 24/7 onsite staff, uninterruptible power and back-up, high tech video surveillance system, biometric security with limited access to certain areas of the facility and only select individuals having administrative access to our servers and databases.

Portal Communications: All data transfer and communication from desktops to the partner portal happens over secured 128/256-bit encrypted connections. We use multi-threat security firewalls which only allow incoming traffic from ports 80 and 443 to enable secure communications.

Remote Access Logs: Remote access to desktops and servers are provided through advanced monitoring and management tools. The tool makes all log history available with timestamps, IP and login credentials.

NOC Access to Domain server: The NetEnrich NOC will utilize a unique, VAR defined Windows domain administrator account to access the NetEnrich NOC managed client servers. All activities completed by the NetEnrich NOC can be verified through security logs.