

InterraIT has a comprehensive, documented Information Security Management framework which defines and implements the information security standards, policies, guidelines, practices as well as review and audit processes across the enterprise. The company follows strict security procedures to ensure total confidentiality and security of operations at its Development Centers (DC). We even encourage our customers to audit our security procedures implemented in their respective DCs at InterraIT-offshore for their satisfaction.

InterraIT has an Information Security (IS) Officer, who is responsible for implementing the security framework in all DCs. IS officer is supported by a 3 member team of security experts who design and implement security procedures at the DCs and also conduct information security audits.

The security policy framework at InterraIT covers all aspects of information security including application, data, network and physical security. The framework consists of security policies spread across four broad categories namely Intranet, Internet, Extranet and Physical Premises.

Intranet security policy covers:

- ▶ Antivirus security
- ▶ Password protection
- ▶ Desktop security
- ▶ Intrusion detection system security
- ▶ Intranet server security
- ▶ Disaster Recovery and Business continuity plan

The Internet security policy covers:

- ▶ Internet access
- ▶ E-mail security
- ▶ Router security
- ▶ Firewall security
- ▶ DMZ security
- ▶ Physical security

Extranet security policy covers:

- ▶ Remote access security
- ▶ Vendor security
- ▶ VPN

Physical security policy covers:

- ▶ Access Control mechanisms
- ▶ Fire Detection
- ▶ Fireproof Storage

Following are the security measures and practices implemented at InterraIT Development Centers

Areas of concern	Security Measures and Practices
<u>Physical Security</u> This refers to chances of a break-in into the development center and losing / stealing of data	<ul style="list-style-type: none"> • Physical security is ensured through the deployment of security personnel. All InterraIT premises are provided with 24x7 physical security • All employees are given electronic access cards for accessing the premises • DC Manager strictly controls movement of media and documents and shares these on a need to know basis • Every person has restricted movement within the development center and is given access to only those systems and areas where he/she is required.
<u>Employee Confidentiality</u> This refers to chances of	<u>Corporate Level</u> <ul style="list-style-type: none"> • To ensure privacy of project data, confidentiality agreements are signed



Corporate Office

USA
 2001 Gateway Place
 Suite-670W,
 San Jose, CA 95110

Development Centers

INDIA
 E-14,
 Special Economic Zone
 Noida, UP 291 305

223 SDF Bldg,
 Sec V, Block GP,
 Kolkata, WB 700 091

USA Offices

Cerritos, CA
 Fullerton, CA
 Dallas, TX
 Columbia, MD

Roseville, CA
 Princeton, NJ
 Oakbrook Terrace, IL
 Bellevue, WA

<p>Information leak and/or Data loss by InterraIT employees</p>	<p>between InterraIT and Customer at the start of every new engagement. As per the mutual agreement InterraIT ensures that confidentiality is maintained about client related information at all times</p> <ul style="list-style-type: none"> It is mandatory for the entire project team to follow the agreed norms <p><u>Project Level</u></p> <ul style="list-style-type: none"> All the employees sign a Non Disclosure Agreement specific to their project Access to proprietary information, critical systems and resources is granted (Information Security) on a need to know basis only, regardless of position or status, through User IDs and password mechanism.
<p><u>Confidentiality of Data</u> This refers to privacy of customer's as well as InterraIT's confidential information and includes protection of Intellectual Property Rights</p>	<ul style="list-style-type: none"> At InterraIT, this is achieved by implementing C2 level security on all servers across the enterprise. A security team deputed for this purpose implements security procedure on all servers and periodically monitors the systems to ensure their adherence to the security policy Movement of any removable media in and out of development center (DC) is restricted.
<p><u>Document security</u> This refers to protection of physical documents in the DC as well as electronic documents residing on the server</p>	<ul style="list-style-type: none"> InterraIT deploys the most stringent encryption standards to provide the highest levels of encryption based security for its data. InterraIT supports two types of VPN connectivity: <ul style="list-style-type: none"> <i>Site to Site VPN</i>: IPsec VPN tunnel is configured with different level of security such as DES, 3DES, AES, which are the latest standards. For message authentication MD5 or SHA1 protocols are used between gateway devices such as firewalls and routers. <i>Client to Site VPN</i>: Standards as above are used between desktop VPN client and VPN gateway at either ends. Access to data stored on hard disks and other devices is strictly controlled through access control lists
<p><u>Network Security</u> This refers to securing the network on which the servers storing the project data are hosted.</p>	<ul style="list-style-type: none"> Each Development Center has a stand-alone network and for security reasons is isolated from the main InterraIT LAN. The connectivity is typically established via extranet site. The entire development is carried on the Application Servers located at DC site only. <p><u>Password Policy</u></p> <ul style="list-style-type: none"> Password policy is implemented and controlled centrally by using windows active directory for all domain controllers and active directory users. Access to network devices is strictly governed by access control matrix and AAA servers using industry standard TACACS+ and RADIUS protocols.
<p><u>Server Security</u> This refers to securing the servers</p>	<ul style="list-style-type: none"> All DC servers are installed within the respective DC area, in an enclosed and secured room. The servers are managed and administered by dedicated system / network administrators assigned for the DC.