Software Product Security Statement for

Integrity Release 3.2

1. INTRODUCTION

As computer systems become more sophisticated, and computer information becomes more accessible, radiotherapy customers are becoming increasingly concerned over potential virus attacks and access to confidential data by unauthorised users. Manufacturers of computer products and network systems in use in hospitals are being required to demonstrate that their products are protected against these potential hazards. Similarly, customers are seeking advice from manufacturers on how best to secure their data.

In response to these demands, Elekta has implemented a procedure and accompanying policy that governs all aspects of the design, installation and use of each of its software products. The policy is transmitted to the customer as a software product security statement which describes the security features provided by Elekta and identifies actions required by the users to assure the security of their own data. Elekta has benchmarked its policy against widely published standards in computer and networking such as HIPAA, NHSNet and IEC 60601-1 to ensure it is addressing relevant issues.

Although care has been taken to ensure Elekta products comply with the software product security statement this document does not act as any form of guarantee.

All software product security statements will be published on the Elekta web site.

2. SOFTWARE SECURITY FEATURES

2.1 Datasets, User Identifiers, Roles and Access Rights

- The information held by this product is classified into a number of datasets. Each dataset is treated separately for security purposes. The datasets include patient data, treatment data, machine settings and the software itself.
- Datasets that are classified as Critical are listed in section 4, together with any additional methods used to ensure their integrity.
- Datasets that are classified as Confidential are listed in section 4, together with any additional security measures protecting access to them. The user roles permitted access to confidential datasets are given.
- Each user of the product needs an individual user identifier (user ID). Each user has a secret password. A user logs onto the product by typing their user ID and password. Significant actions taken by a user are recorded in log files and the user is identified in these log files by their user ID.
- Each user gains access to specific datasets by being given a role.
- Each role gives specific access rights to specific datasets. Each installation needs at least one administrator (a specific role) who creates user IDs, passwords and roles for other users.
- Users may share a role. Users must never share user IDs and passwords; there is no need for them to do so.

2.2 Passwords

This product's software does not require the users to change their passwords on a regular basis, and allows null passwords for legacy users.

This product's software enforces the following rules:

- New passwords are at least 6 characters in length.
- The password cannot be the same as the user ID.

To increase the security of your product, it is recommended that you introduce local procedures that incorporate the following guidelines:

- Users should change their password after their account is created.
- Passwords should be changed at least every 30 days.
- If leaving the control console unattended, the user should "lock" the system by selecting the "Change User" option. This requires a further login to reactivate the system. The system will not automatically "lock" itself when left idle. This requires the user to exit Receive External Prescription application if the system is being used with a 3rd party R&V system.

2.3 Backup & Restore

You are responsible for backing up datasets onto removable media, and for the safe storage of removable media. The mechanism for scheduling automatic backups is defined within the product documentation.

A rigorous tape retention policy is highly recommended. An example of such a policy is:

- Nightly backups to be created, and held for 1 week and then re-used.
- The backups taken on a specific day (e.g. Friday) to be kept for a further month.
- Monthly backups to be maintained for one year.

Removable media used for backup should be clearly labelled.

Ensure that removable media is not used beyond the recommended media life of the manufacturer.

You should nominate someone in your organisation to perform periodic checks of the backup contents, to ensure your disaster recovery procedure is sufficient to restore your system to a known state.

2.4 System Integrity

The system performs an automatic disk integrity check when the system powers up after being shut down abnormally, if the operating system logs indicate a disk write operation may not have been completed correctly. The integrated diagnostic tool allows you to perform an elective disk integrity check.

This product is closed. This means that you can only gain access to its operating system and files through the product. This ensures that the software operates safely and as intended.

2.5 Virus Protection

The main control system software will not scan for viruses, as this is a closed system and there is no virus software installed because it may interfere with the normal operation of treatment delivery. However, virus checking is performed by the NSS software, and is described in the section below.

You can scan installation media for viruses before installing new software in the normal manner on a separate workstation with virus checking software installed.

We scan all media for known viruses before sending it to you.

The Linac Control System cabinet has Microsoft Windows® Embedded Standard (2009) installed with Microsoft Windows® DQI updates up to September 2013. The Windows® Firewall has been enabled on the Linac Control System cabinet. Ports have been enabled to allow correct operation of Integrity. All other ports have been closed. This feature cannot be disabled but can be reconfigured by an authorised user.

2.6 Network Security Solution (NSS)

The Integrity 3.2 product includes the NSS as part of the control system configuration, which provides a number of security features:

- A secure, reliable single-point connection between the Elekta and hospital Networks
- Firewall blocking of all unauthorised network traffic between the Elekta and hospital networks
- Routes connections from the hospital LAN to the correct IP and Port within the Treatment Delivery Suite LAN
- Provides a common backup location for computers within the suite
- Provides checking on the common backup location
- Built-in virus checker

3. YOUR RESPONSIBILITIES FOR SECURITY

In order to use the product's security features effectively, you need to take some actions.

3.1 Installation

You must choose a location for the product where it is secured from unauthorised physical access, and where casual passers-by cannot view confidential information or interfere with the controls.

You must ensure that all network cabling is secured against interference by unauthorised people.

You must not install this software product on a wireless network.

3.2 Networks

The network and NSS must be set up in accordance with the Integrity 3.2 Software Installation Manual.

The specific actions to be taken by your Network Administrator with regard to this software product are:

- Do not grant Administrator or "super user" privileges to user groups that include normal users of the software product.
- Protect the software product from excessive network traffic (averaging at around 20% (+/- 10%) utilisation) by use of a switched network. The use of hubs should be avoided.
- The computer running this software product cannot be used to browse the Internet or other similar 'public' networks.
- If you intend browsing the Internet or public networks from a computer on the network, set up specific user accounts that are clearly defined as having no access to critical operating systems, applications and applications related data. Never allow user accounts with Administrator or "super user" access to browse the Internet.
- It is not possible to use electronic mail software on any computer that runs this software product.
- Connect to the Internet through a firewall that operates on a "deny all" policy. Your firewall should only accept incoming traffic that forms part of an established connection and should restrict outgoing connections to specific ports and specific protocols, for example 80 (http), 443 (https), 53 (dns), 143 (imap), 110 (POP3), 25 (smtp).
- If you are connecting between your hospital and a support site that utilises the Internet or public networks as the communication medium, establish a Virtual Private Network (VPN) between the two sites.
- Set up encryption on any data exchanged through a WAN (such as a Virtual Private Network or any link involving a telephone network). Use the highest level of encryption supported by both ends. Note that encryption above 56-bits is illegal in France.
- The Local Area Network that you have attached the product to, should use non-routable IP addresses as defined in RFC1918 (http://www.isi.edu/in-notes/rfc1918.txt). These are:

10.0.0.0 to 10.255.255.255 (10/8 prefix)

172.16.0.0 to 172.31.255.255 (172.16/12 prefix)

192.168.0.0 to 192.168.255.255 (192.168/16 prefix)

3.3 Remote Support – IntelliMax™

This product can be accessed remotely using IntelliMax™ Connect. Your organisation must nominate at least one support contact. The following security features are designed to provide secure service.

- IntelliMax™ sessions can only be initiated from an IntelliMax™ Gateway PC or an Integrity Control System cabinet.
- IntelliMax™ does not require any inbound ports to be opened at your perimeter firewall.
- We shall not connect to your product without the consent of a nominated support contact.
- Only authorised members of staff with adequate permissions will be able to establish a remote connection.
- Your local service representative will provide the local hospital user with a 6 digit access code. The remote connection will only be established once both the Elekta Service Engineer and the local hospital user have entered the same 6 digit code. This code is session specific and is generated specifically for each remote access session.
- The remote connection is made using encrypted Secure Sockets Layer (SSL) technology.

IntelliMax™ Remote Monitoring will remotely access the Linac Control System cabinet to gather information from the Linac. This information is gathered by an IntelliMax™ Gateway PC, and is transmitted to Elekta's central database using an encrypted Secure Sockets Layer (SSL) connection.

3.4 User ID Administration

Your organisation must appoint at least one administrator. We recommend that your organisation should appoint a deputy administrator to act in the case of absence or emergency.

The duties of administrators include:

- Creating new user IDs and setting their initial passwords.
- Assigning roles to users.
- Investigating failures to log in and re-instating the user's password following an investigation.
- Reviewing logs of users' activities.

4. CRITICAL AND CONFIDENTIAL DATASETS

The datasets considered Critical to the correct operation of the software product are:

Critical Dataset	Additional methods used to ensure integrity (e.g. checksums)
Linac Machine Database	Checksums exist within each file that make up the machine database. These are verified each time that the file is read by the control system. Any failure will set the machine into a safe (non-radiating) state.
Operating System	This is a closed product, meaning that no unauthorised users have access to the operating system. There is a mechanism to gain access through the integrated configuration tool, which can only be accessed by users that know a valid user ID and password.
Integrity Software	The application software files are subject to an independent validation checksum function whenever the console is started. Any files that fail this checksum function will prevent entry into the normal Integrity application. Radiation will not be permitted in this case.

Configuration Information	Configuration data is stored within the operating system registry and the SQL database. Access to both requires the user to have access to a valid user ID and password combination.

The datasets considered Confidential are:

Confidential Dataset	Access protections implemented and user roles permitted access
Linac Machine Database	The only access allowed to these files is through the software product. Any misuse or unauthorised access will be detected by an invalid checksum at next access. Appropriate access in terms of read-only or read-write is given on a per-user basis within the software product. Clinical users can read values, and Service users can write specific values to the database while calibrating the linac, for example.
Operating System	Access to the operating system is only permitted to users that have entered known and valid user Ids and passwords. Independent access to configuration information held within the operating system registry is permitted to suitably authorised users.
Integrity Software	The only method available to write or update the software is through a secure installation mechanism. This requires access to the software installation media and installation instructions from Elekta. Failure during the installation process will prevent normal operation of the Integrity software. Installation engineers are the only user role permitted to change the installed software.

5. APPENDIX A

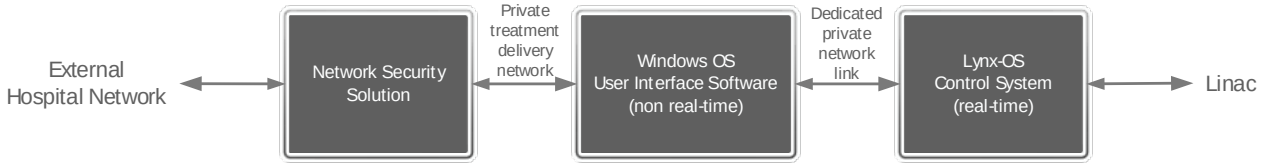
Statement on Virus Vulnerability of Integrity Systems

Integrity has an architecture that makes mistreatments due to virus attacks virtually inconceivable.

Integrity clearly delineates the safety-critical control software

The main architecture has been purposefully designed to ensure that there is a clear separation between the user interface and networking software (running under Windows) and the Linear Accelerator control software (running LynxOS-SE, a real time Operating System).

Treatment delivery is controlled and monitored by the LynxOS real-time control software and associated hardware components, not by the Windows software.



Viruses only affect the Windows software

There is no physical link available for an outside program or virus to connect directly to the real-time control system.

We know of no viruses being circulated that can affect LynxOS-SE (virus writers tend to concentrate on exploiting the Windows OS).

From Integrity R3.0 the Windows system operates in a private network protected from the wider hospital network by the Network Security Solution.

Only Elekta software is ever installed on the Integrity Control System Processor Rack

The only link to the control system is through the Windows programs, which are developed according to Elekta's quality system.

No other software can be installed on the Integrity Control System computers, as it is a closed system - no direct access to the OS is available to users.

Safeguards are built into Desktop prescriptions

Prescriptions for delivery on an Elekta linac must be completely received by Integrity Windows software prior to delivery being allowed to start.

Complete prescriptions are checked for integrity and consistency to ensure only valid and uncorrupted prescriptions can be delivered on an Elekta linac.

All parts of the prescription (geometric and dosimetric) are included in the consistency check performed by Integrity software.

The link between Windows and Lynx-OS has integrity and is secure

All communication between the Windows and LynxOS is made according to a strictly checked protocol.

Any delay in communication between Windows and LynxOS will cause the control system to fail safe (i.e. stop radiation if it has started, prevent it from starting if it has not).

All data passed between the Windows and LynxOS systems have checksums applied and checked.

There are consistency checks made by the control system to ensure that primary and secondary prescribed MU values are valid and consistent.

Virus attacks on Windows will not cause mistreatment

Viruses might infect the Windows side of Integrity, which may cause corruption of data or failure of software processes.

When radiation starts, the Windows side relinquishes control to the real-time control system, and if failures occur on the Windows OS software then no mistreatment will occur.

The LynxOS real-time control software handles beam control and all dosimetric and geometric aspects of the treatment delivery.