Software Product Security Statement for

iViewGT 3.4.1

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.

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

- The user must change their password after it is created
- Passwords should be changed at least every 30 days.
- If leaving the control console unattended, the user should "lock" the system. This requires a further login to reactivate the system. The system will not automatically "lock" itself when left idle.
- The software stores passwords in encrypted form.

2.3 Backup & Restore

You are responsible for backing up and for the safe storage of data. The mechanism for scheduling automatic backups is defined within the product documentation.

A backup 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.

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 product only runs on a dedicated bespoke PC with a specific hardware configuration and therefore cannot be installed on any system. You can only gain access to the Operating System via Windows username and password authentication.

2.5 Virus Protection

There is no virus software installed because it may interfere with the normal operation of iViewGT. 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 viruses before sending it to you.

The iViewGT cabinet has Microsoft Windows® Embedded Standard 7 installed including selected security updates. The Windows® Firewall is enabled on the cabinet. Ports have been enabled to allow correct operation of iViewGT. All other ports have been closed.

2.6 Network Security Solution (NSS)

The iViewGT 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 unauthorized 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

You must provide network connections according to our requirements in the Elekta Oncology Products - Site Planning Computer Hardware, Software & Network Information (Document ID: 1021907).

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.
- It is recommended that the computer running this software product should not 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 a specific user account that is clearly defined as having no access to critical operating system, application and application related data. Never allow user accounts with Administrator or “super user” access to browse the Internet.
- 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.
- It is recommended that you do not use electronic mail software on any computer that runs this software product. If you have enabled e-mail, then configure it to prevent the detaching or execution of executable, scriptable, macro related code or attachments. It is recommended that you use the Netscape/Mozilla suite instead of Microsoft Internet Explorer, to disable any malicious scripting that can be sent via these mediums.
- 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.
- 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)
  192.168.0.0to 192.168.255.255 (192.168/16 prefix)

3.3 Remote Support

3.3.1 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 limit this facility and allow you to maintain control over remote access.

- IntelliMax™ sessions can only be initiated from an IntelliMax™ Gateway PC or an iViewGT 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.

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:

- Operating System
- iViewGT application software
- iViewGT configuration data

The datasets considered Confidential are:

- Patient database

Access to critical and confidential datasets are controlled through normal user access permissions via the host operating system Windows® logins.

Where a central Patient database configuration is used with iViewGT, you must ensure that unauthorized access to the server PC hosting the database is prevented as described in section 3 above.