Software Product Security Statement for

ABC v3.0

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.
- Password protection is achieved via logon to the ABC Laptop. Each user of the product needs an individual user identifier (user ID). Each user has a secret password. A user logs onto the ABC System 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 enforces the following rules:

- Passwords are at least 6 characters in length.

- The user must change their password after it is created or re-instated and 30 days after the last change.
- The password cannot be the same as the user ID
- If a user makes 3 consecutive unsuccessful attempts to log in, that user will be locked out until a suitably authorised user investigates the reason for failure and sets a new password. This limits the number of times an unauthorised person can guess the user's password.
- The Product stores passwords in encrypted form.

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

There is no System Integrity check installed onto this product.

This product is open. This means that you can mount it on a computer of your choice provided that it meets our published specification (Refer to the ABC User Manual supplied with the product for machine specification.) However, we strongly recommend that you dedicate a computer to this software and do not share the computer with other applications.

2.5 Virus Protection

The product does not come with any virus protection software pre-loaded. If you wish, you can install virus protection software of your choosing. In this case, ensure that any automatic checks cannot occur during a clinical treatment.

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

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

This product does not require connection to a Local Area Network in order to operate. It will be documented that Elekta does not recommended that this product be connected to a network.

However, should a hospital need to connect the product to a network, then the following specific actions are to be taken by your Network Administrator:

- 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 strongly 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 strongly 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)
  192.168.0.0 to 192.168.255.255 (192.168/16 prefix)

3.3 Remote Support

Not applicable to this product.

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)
None.	

The datasets considered Confidential are:

Confidential Dataset	Access protections implemented and user roles permitted access
Patient Name	Under the Data Protection Act, and in context of use of equipment at a hospital this data would be considered as Customer Personal Data. The responsibilities of the Supplier (i.e. the hospital) are supported by the approach taken in this SSS, i.e. the system is not networked, it is password protected and each authorised user has unique and personal Ids and passwords. These precautions are considered fit for purpose for an unlimited global release.
Patient hospital ID	Identical consideration as to Patient Name, with the same protection provided.