Dose-X
CyberSecurity Leaflet

The purpose of this leaflet is to provide CyberSecurity information on the Dose-X and software to IT personnel. This information will help ensure the secure and safe use of the system in clinical practice.

What is the system used for?

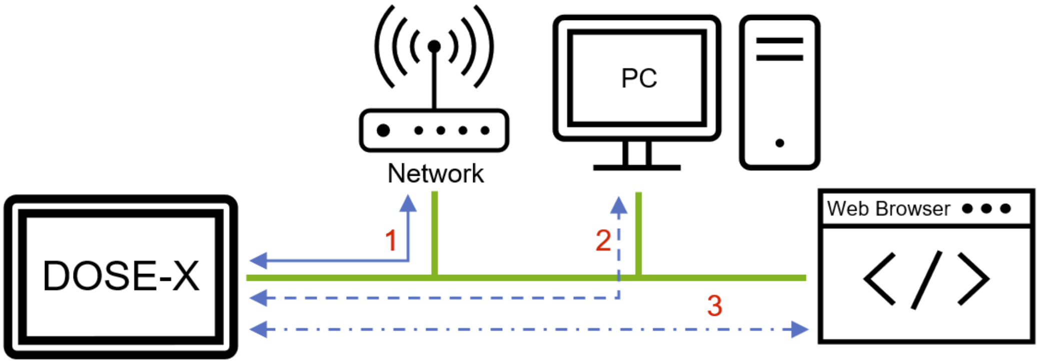
The Dose-X is a high-end, reference class electrometer with added detector and machine libraries, readout capability (dose & dose rate) and triggered (threshold) detection. Control of the Dose-X is handled by a large, touchscreen for fast and easy operation, or over the IT network.

- The purpose of the Dose-X electrometer is reference dose and dose rate measurements in radiation therapy.
- The location of use of the Dose-X is within the premises of a radiotherapy department, near a radiation treatment machine, but not in a publicly accessible space. It is assumed that a high level of physical access control to this area is implemented by the healthcare provider. Consequently, the Dose-X does not implement any particular user authentication; any user who has (physical or remote) access to the instrument is free to use it. Changes related to critical functionality are subject to permission control (authorization) through an admin password. The Dose-X is controlled locally (using the touchscreen), or over the IT network via a web-application on a Tablet or PC, or via software which can directly access API functionality.

What if the electrometer device fails or data is corrupted?

Non-availability of data (or of the whole instrument) does not have a direct effect on patient safety, nor does it cause a security risk. However, patient treatment may be delayed in some situations. It is recommended to the healthcare provider to include non-availability of the device in their risk management for the patient treatment process, *e.g.*, by planning for a backup device or taking other precautions.

How does the system architecture look like?



- 1: The Dose-X can be connected to the local network (Ethernet or Wifi)
- 2: The Dose-X can be connected to a remote PC via a software running on remote PC which can directly access API Functionality of the Dose-X.
- 3: The Dose-X can be remotely controlled via an approved web browser on a Tablet or PC (Ethernet or Wifi).

Are there any operating systems or application software supplied?

- The web application runs on Hardware / OS provided by the hospital IT.
- The Dose-X firmware contains an operating system based on Linux kernel. For updates (including any security patches) firmware files are only supplied by IBA Dosimetry.
- The Dose-X can be controlled remotely via a web browser if it is connected to a network. Using the Dose-X remotely from a web browser other than specified may introduce risks related to the product safety, usability, or CyberSecurity. The following browsers have been tested for remote control:
  - Google Chrome (version 109.0.5414.120 or later)
  - Microsoft Edge (version 109.0.1518.7 or later)

  A remote user signed in as an admin can take away active control of the device from a non-admin user.

What kind of data is stored and handled?

- The measurements taken with the Dose-X are related to a treatment machine rather than to an individual patient. The Dose-X does not handle or store any personal health information (PHI) or other kind of personally identifiable information (PII).
- The admin role and password are not directly attributable to a specific person, since several users can assume this role. There is no other confidential data handled or stored on the instrument.
- The Dose-X stores the following data:
  - device information
  - configuration data
  - user calibration factors
  - measurement history
  - device log files

- The USB port allows the user to:
    - export measurements, libraries, and configuration data
    - import libraries and configuration data
    - install FW upgrades
    - export log files (System log, Measurement log) as plain text which can easily be opened in most text editors and word processors.

- Ports, if remote access is enabled:

80/tcp	http server for the webapp (and API)
443/tcp	https server for the webapp (and API, TLS encrypted)
8081/tcp	webapi over websocket
8083/tcp	webapi over websocket (TLS encrypted)
5353/udp	zeroconf (device discovery)

TLS Certificate

- Usage HTTPS:// with a self-signed certificate may cause security risks

  To provide out-of-the-box functionality, the Dose-X is delivered with the option to either use http:// or https:// with a self-signed certificate for the remote connection. Please note, neither option provides the full level of CyberSecurity and may thus cause security risks**.** We recommend that, if possible, a properly signed TLS certificate is uploaded to the Dose-X. This will suppress the warnings associated with the untrusted self-signed certificate the Dose-X ships and ensures, that the Dose-X devices are properly identified on the IT network.

- The https connection supports TLS 1.2 or 1.3.

Which measures are implemented by IBA Dosimetry to support safe and secure operation?

- An MDS-2 form is published for the Dose-X and are available from our customer support team.
- Our source code is continuously scanned for vulnerabilities. We are employing software to regularly assess and improve the code quality during development.
- For ensuring the authenticity and integrity of firmware updates or upgrades, IBA will provide the SHA-256 checksums via a separate help center article.
- Some system settings and actions are only available to users with admin access (Update firmware, admin settings, network configuration, configuration backup…). Changes to critical functionality (including firmware updates) are protected by a strong password. The password is stored on the device as salted hash.
- Critical data on the instrument (such as calibration or correction factors) are secured with a checksum.
- The admin is able to further improve the security and ensure the identity of the Dose-X device on the IT network by uploading a valid TLS certificate from a trusted provider; thus securing the communication and data transfer between the device and the PC or tablet.
- Direct execution of any executables on the USB stick is technically blocked. Only firmware files and exported libraries / configuration data can be imported.
- Auto-Logoff for admin sessions after a configurable time of inactivity.

Which CyberSecurity measures are expected to be implemented by the operator (health care provider)?

- General requirements expected:
  - State of the art virus scanners and firewalls for the tablet and PC are used.
  - Prescribed maintenance is done as required, including installation of security patches.
  - Windows session timeout for web application session is configured according to local policy.
  - Access control to the medical devices and network access points is established (physically and electronically). Internet access is appropriately protected. Adequate password policy is implemented.
- The Dose-X does not require an internet connection to function, it can be connected via the local network (wired or wireless), and therefore will be part of an environment that is exposed to CyberSecurity threats. This presents a possible security risk. To minimize the chance of an attack IBA recommends the following:
  - Immediately define the admin password.
  - Restrict access by only allowing authorized users to access your network.
  - Use file sharing with caution and avoid sharing over public networks.
  - Ensure your access point software is patched and up-to-date.
  - Firmware Updates provided by IBA should be deployed to provide highest level of security.
  - It is recommended to back up regularly and prior to updates (see Instructions for Use).
- The use of the Dose-X (especially via remote control) on an IT network could result in previously unidentified risks to patients, users, and third parties. It is therefore recommended to the customer’s risk management team, to identify, analyze, evaluate, and control such risks, especially in case of changes to the IT network.
  - Changes in the IT network configuration.
  - Addition of items such as hardware and / or software platforms or software applications to the IT network.
  - Removal of items from the IT network.
  - Upgrades of hardware and / or software platforms or software applications on the IT network.
- While no CyberSecurity issues are known at the time of release of the Dose-X we cannot completely rule out that in the future previously unidentified vulnerabilities or security issues might arise. It is therefore recommended that the customer's risk management team performs a risk assessment related to the use of the Dose-X in the IT network.

We care: what happens in the case of a CyberSecurity incident?

- IBA Dosimetry is available for you 24/7. We welcome any notification about any CyberSecurity event or suspected vulnerability involving IBA hard- or software products.
- Please feel free to call our customer support team or file a request in our helpcenter (see contact information and link below).
- We will handle such reports with high priority, and you will be continuously informed about the progress. If necessary, we will publish a security patch.