GeoSIG Ltd
Wiesenstrasse 39
8952 Schlieren
Switzerland

Tel: +41 44 810 21 50
Fax: +41 44 810 23 50
E-mail: info@geosig.com
Web: www.geosig.com

17. September 2025

GeoSIG Cyber Security Recommendations

GeoSIG instruments, as described in their documentation, have built-in security and safety features against unauthorised access or use. However, ultimately it is the user's responsibility to ensure the safe and secure usage of our instruments based on their actual implementation. No factory delivered solution can fit each and every possible scenario. The user is advised herein that once you connect a device to a network, you are also connecting that network to that device. It is the responsibility of the user to take appropriate precautions so that all devices should be adequately hardened, such as with individual strong passwords, and should have their traffic monitored and managed via appropriate security features, such as firewalls. Also, non-critical devices should be segmented away from networks that contain sensitive information.

Compliance with a well-defined security procedure helps protect not only an individual device, but also other devices connected through the network. Such procedure would be intended to prevent exploitation of an individual device's resources by unauthorized individuals, including the use of such device to attack other systems on the network or the Internet.

The following recommendations can be considered in establishing such a security procedure:

1. Physical access restriction

All devices must be restricted from unauthorised physical access and a well-defined physical access procedure shall be utilised.

2. No Unattended Console Sessions

Except for the devices which are physically secured, no unattended console sessions shall be left running.

3. No Unattended Network Sessions

No unattended user interface sessions shall be left running towards any device accessed through its network interface.

4. Use of a Firewall

For a network that has any connection to the outside world, a hardware firewall must be running and configured to block all inbound traffic that is not explicitly required for the intended use of the network and the connected devices. The user can also consider limiting outbound traffic.

☞ ***Any communication ports that are required for the operation must be protected.***

5. No Unnecessary Services or Ports

If a service or port is not necessary for the intended purpose or operation of the device, that service must not be running and the port must be closed. (e.g. if seedlink server is running, but not used, turn it off)

GeoSIG Ltd
Wiesenstrasse 39
8952 Schlieren
Switzerland

Tel: +41 44 810 21 50
Fax: +41 44 810 23 50
E-mail: info@geosig.com
Web: www.geosig.com

17. September 2025

6. Use of authentication

Network and console device access must require authentication by means of strong and individualised passwords per device (no passe-partout passwords).

Wireless access must require strong encryption to associate (such as WPA2), or some other strong mechanism to keep casual users near the access point from using it to get full access to the network. WEP or MAC address restrictions do not meet this requirement.

7. Password complexity and security

When passwords are used, they must meet the specifications similar to below:

All default passwords must be changed at time of initial access or latest at deployment into service.

Passwords MUST:

contain eight characters or more

contain characters from AT LEAST two of the following three character classes:

```
Alphabetic (e.g., a-z, A-Z)
Numeric (i.e. 0-9)
Punctuation and other characters (e.g., !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
```

8. Privileged Accounts

Privileged and super-user accounts (Administrator, root, etc.) must not be used for non-administrator activities. A secure mechanism to escalate privileges with a standard account is acceptable to meet this requirement. Network services must run under accounts assigned the minimum necessary privileges.

9. No Unencrypted Authentication

All network-based authentication must be strongly encrypted. In particular, insecure services such as Telnet, FTP, SNMP, POP, and IMAP must not be used or must be replaced by their encrypted equivalents.

10. Software / Firmware updates

Networked devices must only run software/firmware that are updated according to supplier's guidelines. A periodical check of any available updates from the supplier must be sought.

Please contact GeoSIG Ltd. if you require any further advice or clarification.