The UK Product Security and Telecommunications Infrastructure (Product Security) regime ("PSTI Act")

We take security very seriously at Phoenix Contact. Read more below on security requirements under the PSTI regime for Phoenix Contact affected products:

Passwords

All passwords of Phoenix Contact products are changeable by the user and that we highly recommend the user should change them.

You can find more information on measures to protect network-capable devices here: Industrial Security Measures. Basic password requirement practice should also be followed, as advised by the UK NCSC. https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

We also have in house Cyber Security specialist offering educational seminars on the importance of these actions. To find out more please contact info@phoenixcontact.co.uk with a Cyber Security request.

Information on how to report security issues.

Any security issues should be reported via https://www.phoenixcontact.com/psirt There is also the email-address psirt@phoenixcontact.com

Information on minimum security update periods

All product security updates are free of charge from Phoenix Contact's website. Please find updates from the downloads section on our product pages and each products support period will be found under additional information.

Product Updates and Vulnerabilities

Phoenix Contact provides our own self reporting portal on product vulnerabilities. https://www.phoenixcontact.com/psirt if you find a product reported already, please follow the instructions on how to mitigate the vulnerability.

This information is only applicable to products sold in the UK.

The above statements are general information and not an official Compliance statement. Each Article if affected will have its own compliance statement found on its product page.