ELECTRONIC TEST & POWER SYSTEMS

CASE STUDY

ETPS (Electronic Test & Power Systems) is a company that specialises in programmable power instruments commonly used for research and performance testing of clean technologies. Given their position within the clean research sector, ETPS felt it was only logical to implement a formal EMS (Environmental Management System) and obtain ISO 14001 certification.

Since implementing ISO 14001, ETPS has experienced a range of benefits. One major benefit is that many purchasing organisations now require suppliers to have ISO 14001 certification as standard protocol. As a result, when asked if they comply with the standard, ETPS can now simply provide their certificate, rather than filling out multiple forms and answering a range of questions to provide evidence that they meet the buying organisation’s supplier criteria. This saves the company a significant amount of time over a number of years.

In addition, having ISO 14001 certification reinforces ETPS's commitment to rigorous quality standards to customers who demand the highest quality. The company works with many of the world's leading technology brands, providing them with the tools to innovate. With ISO 14001 accreditation, ETPS can provide added assurance to these customers that they are committed to environmental sustainability and responsible business practices.

When asked what advice they would give to other organisations considering implementing ISO 14001, ETPS emphasised the importance of creating a management system that streamlines company processes. Instead of simply checking boxes to achieve compliance, companies should use the process as an opportunity to assess existing systems at every point and ask, "can we do this better?" By challenging existing processes and striving for continuous improvement, companies can reap the full benefits of ISO 14001 certification and achieve a more efficient and sustainable business model.

•**A.8.12 Data leakage prevention**

Organisation's need to: -

- Classify data in line with recognised industry standards (PII, commercial data, product information), in order to assign varying risk levels across the board.
- Closely monitor known data channels that are heavily utilised and prone to leakage (e.g. emails, internal and external file transfers, USB devices).
- Initiative-taking measures to prevent data from being leaked, through sticked file permissions and adequate authorisation techniques.
- Restrict a user's ability to copy and paste data (where applicable) to and from specific platforms and systems.
- Require authorisation from the data owner prior to any mass exports being carried out.
- Consider managing or preventing users from taking screenshots or photographing monitors that display protected data types.
- Encrypt backups that contain sensitive information.
- Formulate gateway security measures and leakage prevention measures that safeguard against external factors such as (but not limited to) industrial espionage, sabotage, commercial interference, and/or IP theft.

•A.8.16 - Monitoring activities

It is immensely important for organisations to promote a proactive approach to monitoring and ensure that it aims to prevent incidents before they happen, and works in conjunction with reactive efforts to form an end-to-end information security and incident resolution strategy that ticks every box

•A.8.23 - Web filtering

This control is a preventive type of control that requires organisations to put in place appropriate access controls and measures to prevent access to malicious content on external websites.

•A.8.28 - Secure coding

Requires organisations to establish and implement organisation-wide processes/procedures that cover secure coding that applies to both software products obtained from external parties and to open-source software components. It must also keep up to date with ever changing real-world security threats and with the most up-to-date information on known or potential software security vulnerabilities. This will help organisations to improve and implement robust secure software coding principles that are effective against evolving cyber threats.

The 27001-2013 version has 14 sections that detailed the 114 controls and these have been changed in the 27001-2022 standards to the 4 sections below.

NEW ISO 27002 HAS 93 CONTROLS IN THE FOLLOWING 4 SECTIONS

- **Organizational controls (clause 5)**
- **People controls (clause 6)**
- **Physical controls (clause 7)**
- **Technological controls (clause 8)**