STORMSHIELD

CYBERSECURITY COMPLIANCE FOR ENERGY ORGANIZATIONS

In the energy sector, where distribution is absolutely vital, a cyberattack can have a domino effect on the economy, as the entire planet—from stock exchanges and hospitals to factories and nuclear plants—depends on energy.
A cyberattack can have a major financial impact on the affected organization and its customers. However, the most widespread impacts are the result of situations where everyone is connected to a single network. A vivid example is the Industroyer attack, which paralysed Ukraine's power grid in 2016.
A cyberattack can also have major environmental impacts, as all energy facilities (such as coal plants, oil drilling and exploration rigs, offshore platforms, etc.) carry a major risk of environmental damage. These risks are multiplied many times over in the case of nuclear energy.

> EUROPEAN REGULATIONS: COMPLIANCE REQUIRED

> COMPLIANCE OPTIONAL

> COUNTRY-SPECIFIC REGULATIONS

> FOR EVERY PROBLEM, THERE'S A STORMSHIELD SOLUTION

> COMPLIANCE IS NOT ENOUGH

> EUROPEAN REGULATIONS: COMPLIANCE REQUIRED

Organizations in the energy sector are required to comply with the following European cybersecurity regulations:

General Data Protection Regulation (GDPR)

The GDPR is an EU regulation designed to harmonize data privacy laws across Europe, protect and empower all EU citizens as regards their data privacy, and reshape the way organizations approach data privacy. This creates new constraints and requirements for IT managers, CIOs and CISOs.

Key among these requirements is “data protection by default,” which stipulates the protection of personal data as a default property of systems and services. Stormshield products help organizations comply with these requirements by increasing the cyber resilience of their infrastructure. Moreover, Stormshield Data Security provides data-encryption capabilities, which the GDPR mentions as an appropriate technical measure for ensuring the level of security appropriate to the risk.

Network and Information Security Directive (NIS)

The NIS Directive, the first EU-wide legislation on cybersecurity, is designed to boost the overall level of cybersecurity in the EU, and must be transposed into the law of each member state. Under the NIS, each country must designate Operators of Essentials Services (OESs) in sectors such as energy, transportation, water, banking, healthcare and digital infrastructure. Designated OESs must then comply with the Directive.

Certified, trusted Stormshield products enable OESs to deploy security solutions that increase the protection level of Essential Information Systems (EIS). For example, Stormshield Network Security can isolate network areas, enable secure remote access, authenticate users and manage vulnerabilities. Stormshield Endpoint Security (SES), working alongside an antivirus (if any), provides in-depth workstation protection against sophisticated threats. SES can also enhance the protection of legacy operating systems, detect and manage incidents, and protect against bounce attacks.

Payment Card Industry Data Security Standard (PCI-DSS)

The PCI-DSS is a set of information security standards for organizations that handle branded credit cards issued by the major credit card companies. Every merchant, financial institution or other entity that stores, processes or transmits cardholder data must comply with these standards, which include provisions for network security, data encryption, vulnerability management and strong access control.

Stormshield products enable organizations to comply with many of the main PCI-DSS requirements. For example, Stormshield Network Security (SNS) can isolate network areas and encrypt outgoing traffic, manage vulnerabilities and authenticate users. Stormshield Data Security (SDS) can encrypt cardholder data to ensure data integrity and confidentiality. Stormshield Endpoint Security (SES), working with an antivirus, strengthens workstation protection against advanced threats. SES can also enhance the protection of legacy operating systems, detect and manage incidents, and protect against bounce attacks.

> EUROPEAN REGULATIONS: COMPLIANCE REQUIRED

Directive on the Re-Use of Public Sector Information (PSI)

The PSI Directive establishes a common legislative framework that encourages EU member states to make as much public sector information available for re-use as possible. PSI includes all information that public bodies produce, collect or pay for. The PSI Directive, as transposed into the laws of each country, is the basis for the EU's Open Data Policy. All organizations that manage public information or generate data from publicly funded research projects must provide public access to these data, subject to certain constraints.

Stormshield products can help organizations comply with the PSI directive. In particular, Stormshield Network Security (SNS) enables micro-segmentation of the network, so the public data storage area can be isolated. And, with its intuitive security policy management, SNS makes it easy to identify network areas, manage access by user or by group, and institute timing restrictions.

IEC 62443

The ISA-99/IEC 62443 standard, created by the International Society of Automation, is the worldwide standard for industrial control systems (ICS) and is designed to deal with the increasing volume of cyber threats. The standard enables organizations to improve the digital safety and security of their processes and control systems, such as DCS, PLC, SCADA, etc. The standard is derived from the ISO/IEC 27000-series and has been fully adapted to focus on industrial control system environments.

Enhancing cybersecurity is a multi-layered task, and includes governance, security policies and organizational procedures. In this context, Stormshield's highly trusted solutions, which are certified EU Restricted, can help organizations protect themselves from cyber threats.

For instance, Stormshield Network Security (SNS) can isolate network areas, control PLC commands and secure remote maintenance access. Moreover, Stormshield Endpoint Security (SES), working alongside an antivirus (if any), provides in-depth workstation protection against sophisticated threats. SES can also enhance the protection of legacy operating systems, detect and manage incidents, and protect against bounce attacks.

Cybersecurity Act

The European Cybersecurity Act is a response to the growing threat of cyber-attacks that strengthens the prerogatives of the European Union Agency for Cybersecurity (ENISA) and establishes a European framework for cybersecurity certification. The European framework for cybersecurity certification seeks to strengthen the security of connected products, Internet of Things devices and critical infrastructures through certificates. This certification of products, processes and services will be valid in all Member States. The three levels ("Basic", "Substantial" and "High") will help users identify the guaranteed level of security and will ensure that security aspects will have been independently identified.

Stormshield products have already reached the "Standard Qualification" level awarded by French cybersecurity agency ANSSI. Given that the European framework's "High" level corresponds to ANSSI's "Basic Qualification" level–which is below the "Standard Qualification" level–Stormshield products already meet ENISA's expectations in terms of cybersecurity.

Want to take an even deeper dive? Here goes!

> COMPLIANCE OPTIONAL

Energy organizations may wish to comply with the following standards to improve their level of cybersecurity, although compliance is not required under current legislation.

Common Criteria / Evaluation Assurance Levels (EAL3+, EAL4+, etc.)

Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) for computer security certification. It provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous, standard and repeatable manner at a level that is commensurate with the target environment for use. Under this standard, the product's Evaluation Assurance Level (EAL3+, EAL4+, etc.) indicates how thoroughly the product (e.g., a firewall) has been tested. This certification is recognised by some 30 countries worldwide, in Europe, North America, Asia and the Middle East.

Stormshield products are not merely certified to Common Criteria standards: they have achieved the much higher "Standard Qualification" level issued by the National Cybersecurity Agency of France (ANSSI).

To achieve this highly trusted status, the product must:
- Obtain high-level certification with a security target that was defined and validated by ANSSI,
- Withstand additional analysis carried out by ANSSI, including an audit of the product's source code.

Note that "Standard Qualification" is a prerequisite for a product to receive the "NATO Restricted" or "EU Restricted" label required for handling classified information.

ISO/IEC 27000 Information technology – Security techniques – Information Security Management Systems

The ISO/IEC 27000-series is a family of information security standards that provides a globally recognised framework for best-practice information security management. Deliberately broad in scope, the series is applicable to organizations of any size, in any industry. The information security management system (ISMS) provides a systematic approach to keeping sensitive infrastructure secure. Given the dynamic nature of information risk and security, the ISMS concept incorporates continuous feedback and improvement to respond to changes in threats, vulnerabilities or impacts of incidents.

Stormshield products are designed to keep sensitive infrastructure secure. A standard log format enables organizations to centralize all information, so as to identify trends and potential security vulnerabilities. A highly intuitive GUI enables users to easily implement improvements.

> COUNTRY-SPECIFIC REGULATIONS

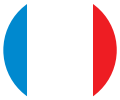
UNITED KINGDOM

Data Protection Act 2018

Similar to GDPR, the Data Protection Act is specific for the United-Kingdom. It states for any personal data, there should be "an appropriate level of protection" depending on the risks involved if there is a security breach. This includes a level of security to prevent unauthorized or unlawful processing, accidental loss, destruction or damage to the data.

Stormshield products help organizations comply with these requirements by increasing the cyber resilience of their infrastructure. Moreover, Stormshield Data Security provides data-encryption capabilities, which the GDPR mentions as an appropriate technical measure for ensuring the level of security appropriate to the risk

> COUNTRY-SPECIFIC REGULATIONS



FRANCE

The Military Planning Law (MPL)

The "Loi de Programmation Militaire" (the LPM or 'Military Planning Law ') lays down guidelines concerning France's defence policy. Faced with the increasing number of cyberattacks carried out by hackers, terrorists or even hostile states, ensuring the cyber resilience of the IT systems of Operators of Vital Importance (OIV) is a clearly defined theme of the MPL. It therefore includes a cybersecurity aspect and lists the OIV in 12 activity sectors, including the energy sector.

With them all approved by the ANSSI (the National Cybersecurity Agency of France), this trust and confidence in Stormshield products enables the OIV to deploy these security solutions to improve the level of protection afforded to critical information systems. As an example, Stormshield Network Security ensures network segmentation, security for remote access, user authentication and vulnerability management. Deployed in combination with an antivirus system, Stormshield Endpoint Security (SES) proposes in-depth protection for workstations against sophisticated attacks. SES can also improve the security of obsolete operating systems by detecting and managing incidents and providing protection against Smurf attacks.

The ANSSI Guide to Good Practices

The National Cybersecurity Agency of France (Agence Nationale de la Sécurité des Systèmes d'Information - ANSSI) is an organisation which operates as a genuine driving force for cybersecurity in France and which regularly produces guides to good practices. These are not actually regulations but rather decision-making aids to be used when selecting service providers and when choosing or deploying cybersecurity solutions. An extensive range of fascinating documentation is available, covering subjects ranging from workstation cryptology to networks.

> COUNTRY-SPECIFIC REGULATIONS

GERMANY

Standards of the Federal Office for Information Security (BSI)

The BSI standards are an elementary component of the IT-Grundschutz methodology. The current BSI standards are:

- 200-1 (General requirements for an information security management system)
- 200-2 (Basis for the development of a solid information security management)
- 200-3 (All risk-related steps in the implementation of basic IT protection)

IT Security Act (IT-Sicherheitsgesetz) & BSI Act (BSI-Gesetz)

According to the IT Security Act, the energy operators must comply with a minimum level of IT security and report significant IT disruptions to the BSI. With regard to the minimum level, Section 8a of the BSI Act was enacted by the IT Security Act, which describes the requirements for operators of energy supply networks or energy plants. In addition, in 2016 the BSI-Kritisverordnung was adopted to specify which critical systems are to fall under the provisions of the IT Security Act. Section 2 of the BSI-Kritisverordnung stipulates that the supply of electricity, gas, fuel and heating oil and district heating are to be regarded as critical services.

Certified, trusted Stormshield products enable to deploy security solutions that increase the protection level of IT systems. For example, Stormshield Network Security can isolate network areas, enable secure remote access, authenticate users and manage vulnerabilities. Stormshield Endpoint Security (SES), working alongside an antivirus (if any), provides in-depth workstation protection against sophisticated threats. SES can also enhance the protection of legacy operating systems; detect and manage incidents; and protect against bounce attacks. Stormshield Data Security helps to prevent data leakage by ciphering sensitive information.

Energy Industry Act (EnWG)

Section 11 (1a) EnWG specifies the requirements for a secure energy supply network with regard to IT requirements. Section 11 (1b) sentence 1 EnWG accordingly obliges operators of energy systems that have been designated as critical infrastructure to provide adequate protection against threats to telecommunications and electronic data processing systems used for network control.

Certified, trusted Stormshield products enable OESs to deploy security solutions that increase the protection level of essential information systems (EIS). For example, Stormshield Network Security can isolate network areas, enable secure remote access, authenticate users and manage vulnerabilities.

> COUNTRY-SPECIFIC REGULATIONS

GERMANY

Atomic Energy Act (AtG)

The Information Security Management System (ISMS) provides a systematic approach to keeping sensitive infrastructure secure. Given the dynamic nature of information risk and security, the ISMS concept incorporates continuous feedback and improvement to respond to changes in threats, vulnerabilities or impacts of incidents.

Stormshield products are designed to keep sensitive infrastructure secure. A standard log format enables organizations to centralize all information, so as to identify trends and potential security vulnerabilities. A highly intuitive GUI enables users to easily implement improvements.

Safety catalogues Federal Network Agency

The Federal Network Agency has the task, in consultation with the Federal Office for Information Security (BSI), of drawing up and publishing minimum standards for IT security in the energy sector. These minimum IT security standards have been published for the energy sector in the so-called "IT security catalogues".

> COUNTRY-SPECIFIC REGULATIONS

ITALY

Directive 1 agosto 2015 (National Framework for Cybersecurity enforcement)

The Directive enforces objectives set out with the National Framework for cybersecurity, empowering coordination among public administration entities as well as partnership with all non-public operators which control IT and telematic infrastructures considered critical functions at national level. The Directive assigns to the Agenzia per l'Italia Digitale (AgiD) the task of developing standards for administrations.

Law decree 18 maggio 2018, n. 65 (Implementation of the directive (EU) 2016/1148 - NIS)

The Law establishes measures for a security at national level, including the establishment of CSIRT (also known as CIRT), duties of the s.c. "critical market operators" and digital providers on security breach procedures, international cooperation on security issues and the adoption of a national cybersecurity strategy.

Certified, trusted Stormshield products enable OESs to deploy security solutions that increase the protection level of Essential Information Systems (EIS). For example, Stormshield Network Security can isolate network areas, enable secure remote access, authenticate users and manage vulnerabilities. Stormshield Endpoint Security (SES), working alongside an antivirus (if any), provides in-depth workstation protection against sophisticated threats. SES can also enhance the protection of legacy operating systems; detect and manage incidents; and protect against sophisticated attacks.

D.P.C.M. 17 febbraio 2017 (Orientation on National information technology security and cybersecurity - Gentiloni Decree)

The Directive establishes the institutional organization in charge of national IT security and cybersecurity, setting out duties and responsibilities of each entity (CISR, CISR Tecnico, DIS role and guidelines, Nucleo per la Sicurezza Cibernetica and its duties). The Directive establishes also measures to "critical market operators" as well as Communication Providers.

> COUNTRY-SPECIFIC REGULATIONS

ITALY

D.P.C.M. 27 gennaio 2014 (National Strategy Framework for Cybernetic space - QSN)

The National Strategy Framework for Cybernetic space aims to ensure the efficiency and the interoperability of assets devoted to common defence, and supporting the full integration of the cyber domain in NATO defence planning process and in the military doctrine, so as to ensure the deployment of a robust capability against cyberattacks.

Stormshield Network Security has been awarded NATO Restricted and EU Restricted certifications. As such, these products can be deployed in sensitive environments to provide secure transmission of classified information. This helps to guarantee international interoperability with NATO and EU institutions.

> COUNTRY-SPECIFIC REGULATIONS

SPAIN

PIC Law (Protection of Public Infrastructures - Ley PIC)

The Critical Infrastructure Protection Law (Ley PIC 8/2011) is complemented by Royal Decree 704/2011. The two main objectives of this standard are: to catalogue the set of infrastructures that provide essential services to our society and to design a plan that contains measures of prevention and effective protection against possible threats to such infrastructures, both in terms of physical security and in terms of the security of information and communication technologies.

Certified, trusted Stormshield products enable critical infrastructure to deploy security solutions that increase the protection level of essential information systems.
For example, Stormshield Network Security can isolate network areas, enable secure remote access, authenticate users and manage vulnerabilities. Stormshield Endpoint Security (SES), working alongside an antivirus (if any), provides in-depth workstation protection against sophisticated threats.
SES can also enhance the protection of legacy operating systems; detect and manage incidents; and protect against bounce attacks.

National Security Scheme, Royal Decree 3/2010, of 8 January

This plan applies to any public utility company for energy and water, as well as any private company that provides services to these companies.

Stormshield products help organizations comply with this scheme by increasing the cyber resilience of their infrastructure. Stormshield Network Security ensures edge protection with Unified Threats Management features. Our SNS range is also the only European range certified "Productos Cualificados" and the only range of firewalls certified "Productos Aprobados" by the Spanish National Cryptology Centre (CCN). Additionally, Stormshield Endpoint Security increases the security level of traditional antivirus by blocking advanced threats. Finally, Stormshield Data Security provides data-encryption capabilities, which is an appropriate technical measure for ensuring the level of security appropriate to the risk.

> FOR EVERY PROBLEM, THERE'S A STORMSHIELD SOLUTION.

Stormshield products and solutions for the energy industry

> COMPLIANCE IS NOT ENOUGH

The vast number of regulations and standards has become a real headache for all organizations. While this guide provides perspective on which regulations apply to each industry, compliance is not enough. It's crucial to remember that every organization needs to map and manage its risks to ensure its own security.