SATEC

EXPERTPOWER CYBERSECURITY POLICY

One of the most valuable assets of every organization or person is always the data related to organizational strategies, intellectual properties, behavior patterns, finance, etc.

For decades,these assets were recorded on paper and stored in locked vaults of the organizations, or third party companies offering storage services. In today's world, digital data is exchanged by different interfaces and stored in various local and cloud digital storages.

Cybersecurity is a constantly evolving process on the part of the data storage service companies to keep up to date with the most efficient cybersecurity tools, repeating inspections, and strict policies that vary from segment to segment, and are based on different project needs.

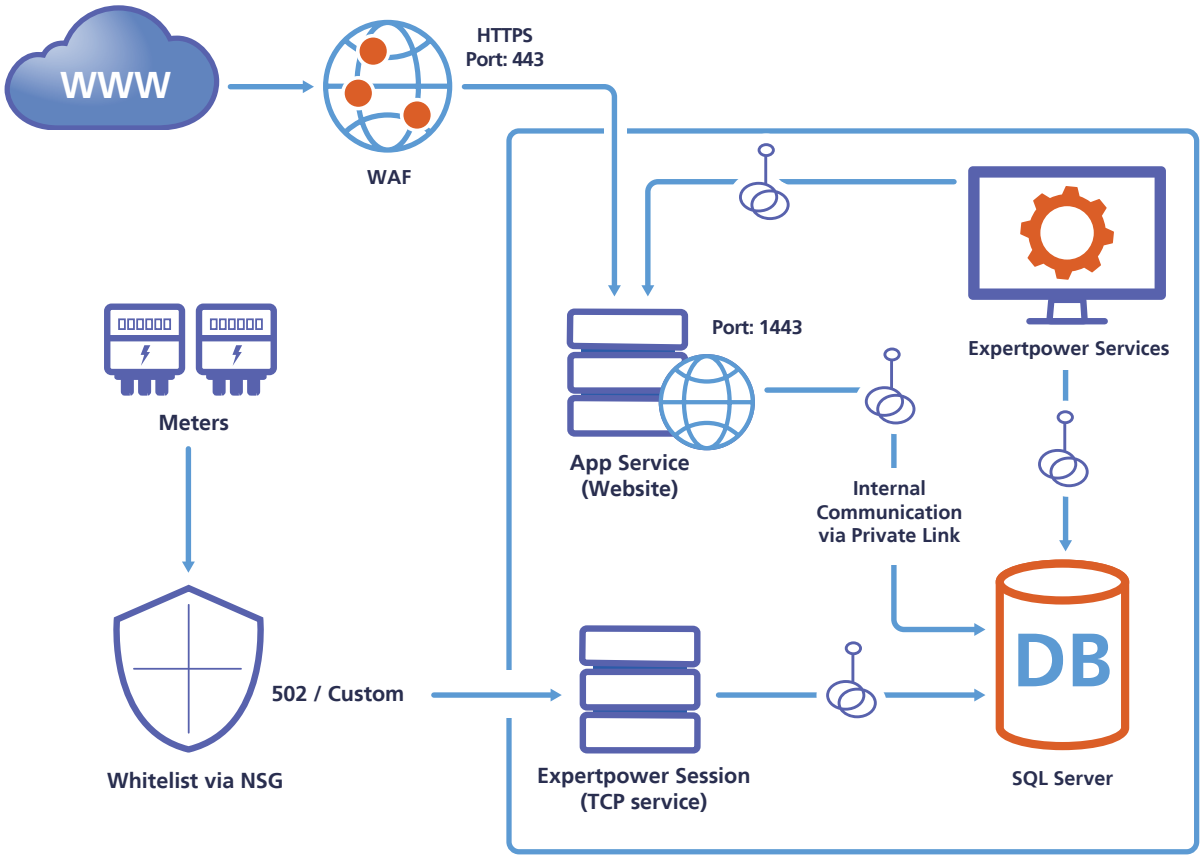
Expertpower is a state-of-the-art solution, with its core activity being the Meter Data Management application. Our goal is to deliver this high-end MDM service in the most secure way - by protecting all the data and privacy rights from inappropriate access or usage. In addition, we comply with the strictest privacy policies in the market, as well as specific client requirements.

Expertpower is designed to meet the security strategy, which follows the global industrial automation control system security standards. A defense-in-depth strategy is a multilayered approach to cybersecurity, with intentional redundancies to increase the security of a system.

The platform security layers can be described as:

- Data Layer (includes access control and encryption of data)
- Application Layer-application hardening
- Host Layer (includes patch implementation user authentication)
- Network Layer includes tools such as IPsec, WAF and network segmentation
- Perimeter Layer (includes firewalls, VPN)

Expertpower - Cloud setup



As a part of Expertpower's cyber security policy, the following activities are taken to withstand the constantly evolving cyber threats, as well as the different privacy policies:

1

ISO 27001

By acting accordingly and complying with the requirements of this standard, we address a very long list of elements and layers of security, starting from secure development environments and processes, Human Resources related topics, infrastructure security of the sites and application, privacy policies of different users, and other aspects.

2

Penetration Tests

Penetration Tests are performed by third-party companies on an annual basis to inspect Expertpower security on the application level, based on the 10 OWASP approach, identifying possible weak spots and potential threats. Due to these repeating tests performed by third party cybersecurity experts, the system is constantly updated, and potential weak spots or threats are eliminated upfront. A few examples of the applied tests and affected environments are listed below:

- Brute Force Attack
- Insecure Direct Object Reference (IDOR)
- HTML Injection Attack
- Development Environment
- Communication
- Sensitive Information Disclosure

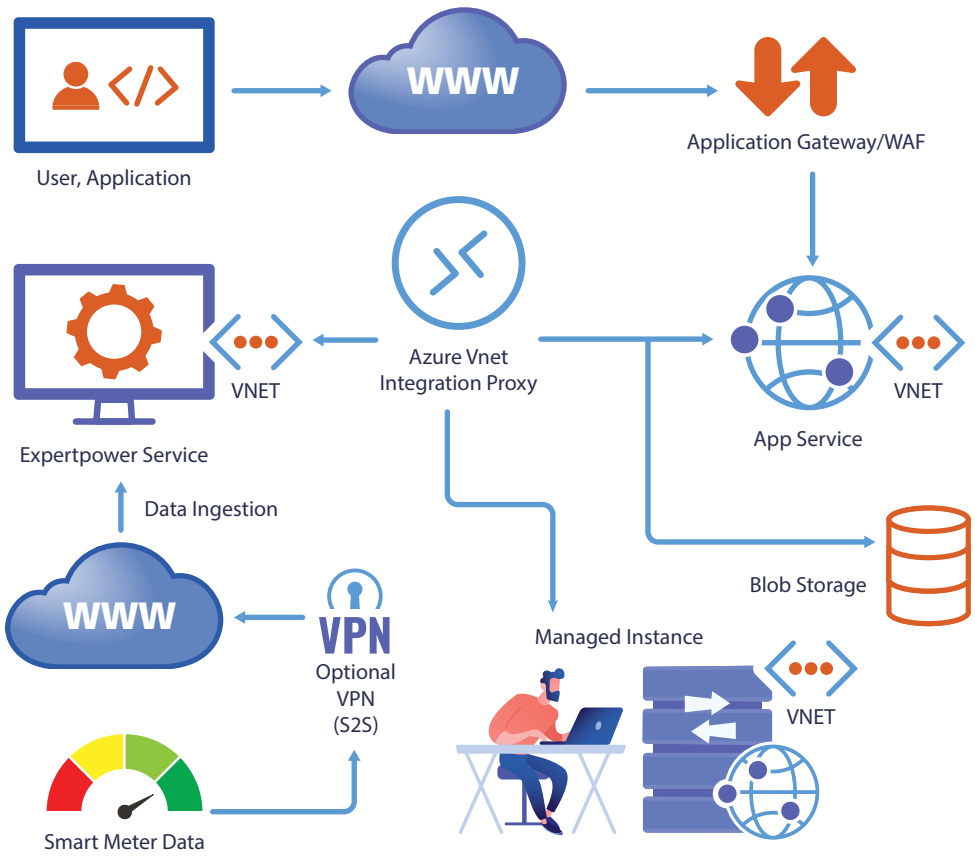
SATEC

3 Data Flow and Platform Deployment

The data collection process, whether from IoT devices or third-party systems, is performed by concurrently running different internal secure processes of data authentication of the source (preventing unwanted users from pretending to be a data source), and others.
The platform includes features such as data encryption using SHA-512 and AES-256 cryptography (At Rest) and TLS 1.2 / HTTPS (In Transit), compatibility with antivirus and whitelisting software user account management.

In addition, there are options to use session timeout of inactive user sessions and advanced encrypted VPN connections, which can be applied in parallel to the application and server protection layers, and a way to secure the data flow on its way to the platform.

Expertpower AZURE Deployment Diagram



SATEC

4

Leveraging the Cloud

By implementing a cloud solution, the users benefit from highly resilient, always up-to-date security capabilities and practices, as well as a very scalable solution, which harvests the power of the cloud resources to minimize downtime risks or extreme overloading of data transfers. In addition, the cloud hosting service providers support our security efforts with their protection layers, making our combined security approach even more powerful and effective.

5

Company Data Validity and Availability Policy

This policy establishes guidelines for ensuring the validity and availability of company data, by outlining the responsibilities, procedures, and safeguards necessary to maintain the accuracy, integrity, and accessibility of critical data assets. The policy applies to all employees, contractors, and third-party vendors who may need access to company data for service needs, including but not limited to:

- Employee records
- Financial data
- Customer information
- Product/service details
- Intellectual property

All employees are responsible for ensuring the accuracy of the data they handle. This includes verifying data prior to insertion into company systems and promptly correcting discrepancies or errors.
Any automated systems or software used to input, store, or process company data must have validation mechanisms to prevent incorrect or incomplete information entry. Regular audits and checks will be conducted to verify the accuracy and validity of critical data. These audits may be performed by internal or external auditors, as designated by the company.

Obsolete or outdated data will be identified and disposed of following company data

retention policies to ensure that only valid and relevant information is retained. Critical data will be regularly backed up and stored in secure, off-site locations.
Access to sensitive and critical data will be restricted to authorized personnel only. Access permissions will be assigned based on the principle of least privilege.
A comprehensive disaster recovery plan will be maintained to swiftly recover data and restore operations in the event of a catastrophic event or system failure.

Systems and data availability will be actively monitored, and any anomalies or disruptions will be reported and addressed promptly.
All employees will receive training on data validity and availability, and the specific procedures and tools to maintain these attributes.
Non-compliance with this policy might result in disciplinary action, including termination of employment and legal penalties under applicable laws and regulations.
This policy will be reviewed annually to ensure its effectiveness and relevance.

6 User Management & Access Permissions

Access to every module menu, or acting as the Expertpower platform, can easily be controlled based on the required user access and permission levels. All permissions and roles are defined during the commissioning stages of theproject, and later can easily be reassigned to new users. Such distributed access to the system is easy to set up and manage, while preventing unauthorized activities or access to other users' data.