1P360S

Driving Innovation

# Leverage the 1P360S Platform to guarantee full compliance with the NIS2 Directive

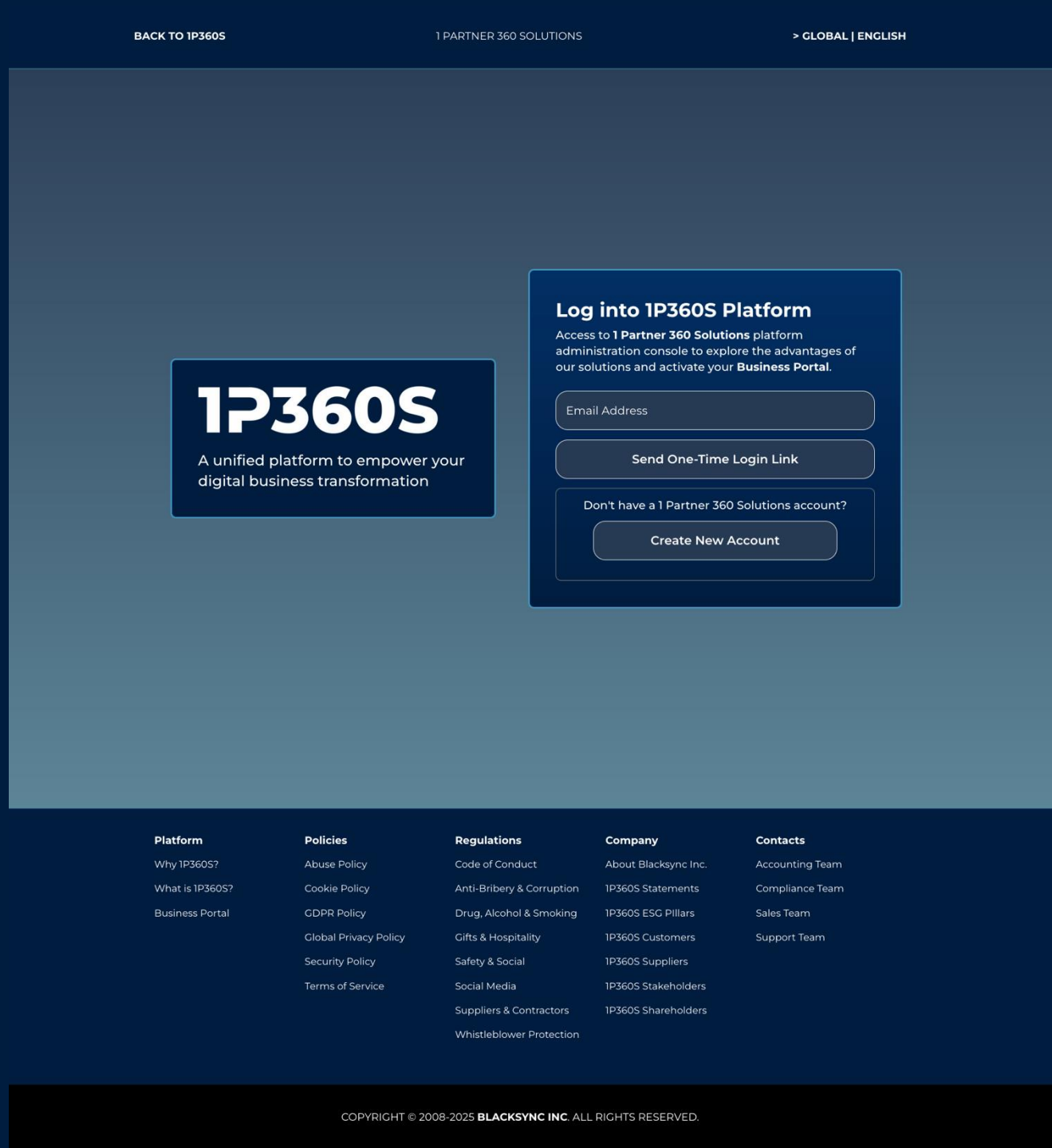
# 1P360S

## & NIS2 Directive

## 1 Partner 360 Solutions

W: www.1p360s.com

For any additional information
you can contact us by email at
sales@1p360s.com



01

# NIS2 Directive

The new European directive on cybersecurity

01

## European Union & Cybersecurity

The NIS 2 Directive represents a significant advancement in the European Union's policy on cybersecurity. Building upon the foundations established by the NIS Directive, the NIS 2 Directive aims to create a uniformly high level of cybersecurity across the Member States in response to the increasing sophistication and frequency of cyber threats. This directive broadens the range of its regulations, enhances security and incident reporting requirements, and introduces more rigorous enforcement measures, all intending to promote improved cybersecurity practices among essential entities.

The scope of the NIS 2 Directive has been expanded to encompass a broader range of industries and entities. In contrast to the original NIS Directive, which primarily targeted critical sectors such as energy, transport, banking, and health, NIS 2 includes additional industries, specifically waste management, the manufacturing of essential products, space, public administration, and digital infrastructure providers, including content delivery networks and social networking platforms.

# Organizations impacted by NIS2

### Essential Sectors and Entities

The NIS2 Directive impacts various public and private organizations that deliver essential services or infrastructure or engage in activities within the European Union. The directive distinguishes organizations and industries into Essential Sectors of High Criticality such as Energy: electricity, district heating and cooling, oil, gas. Transport: air, rail, water, road. Banking. Financial Market Infrastructures. Health Systems. Water: drinking water, wastewater. Digital Infrastructure. ICT Service Management (B2B). Public Administration. Space.
Essential entities, varies by sectors but in general referred to those with more than 250 employees and annual turnover of Euro 50 million and above.

### Critical Sectors & Important Entities

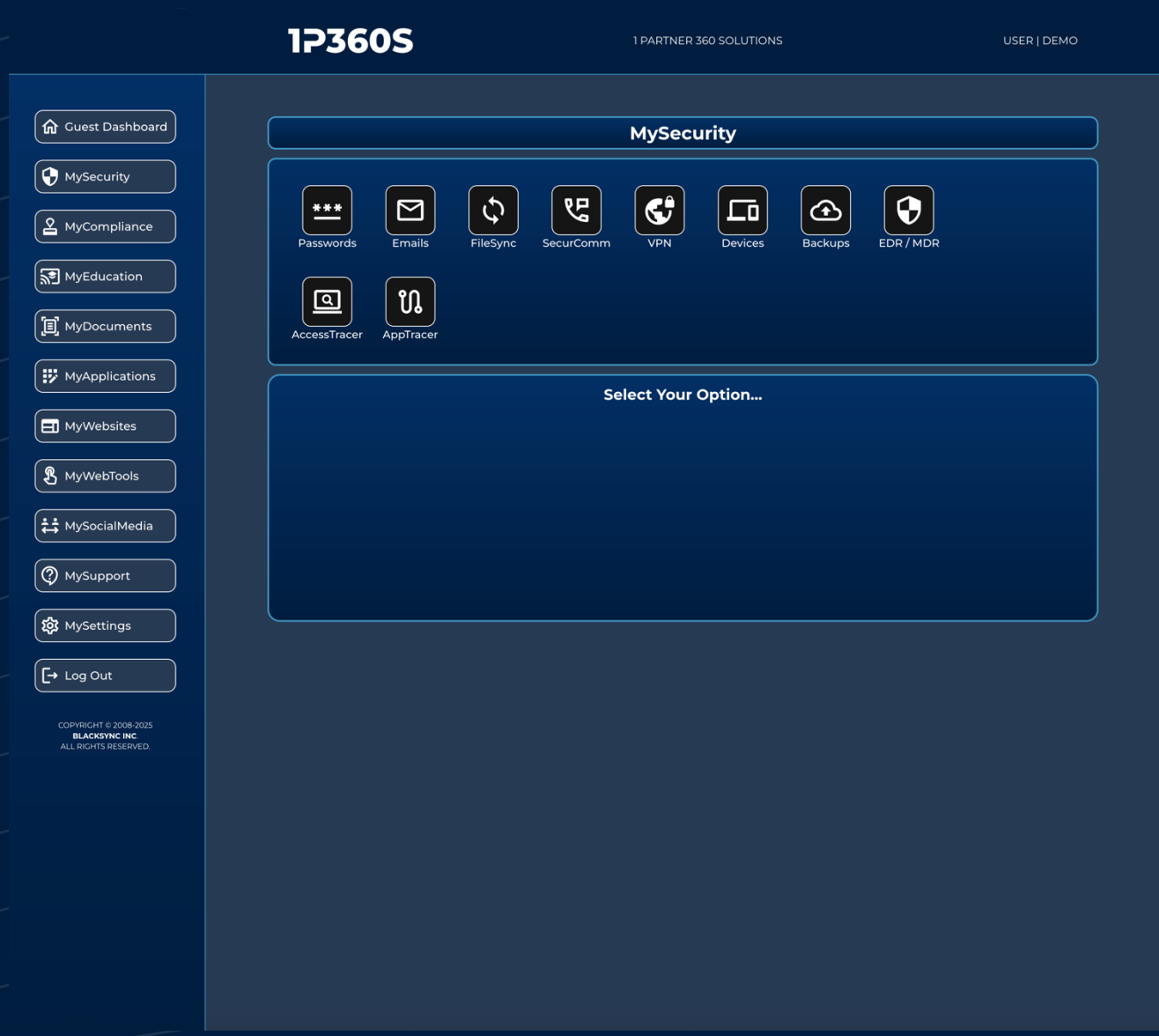
Important entities exhibit variability across different sectors but generally operate under a lower threshold. Such entities are characterized by having more than 50 employees and an annual turnover exceeding 10 million euros. The critical sectors are Postal and Courier Services, Waste Management, Manufacture, Production and Distribution of Chemicals Production, Processing and Distribution of Food Manufacturing, Medical Devices, Computer Electronic or Optical Products, Machinery, Vehicles Digital Providers Research

### Other Entities

It is important to note that, in addition to entities classified within essential and critical sectors and significant enterprises, any company, regardless of size, may be designated as an obligated subject if specific criteria are satisfied. For instance, a company may be identified as essential if it is the sole provider of services deemed critical or necessary. Furthermore, organizations that maintain supply relationships with entities obligated under the NIS2 directive may be required to implement specific provisions, albeit less stringent.

# Risk Management

Comprehensive cybersecurity measures



# MySecurity for risk management

## Cybersecurity Risk Management

By the NIS Directive - Article 21, Member States must ensure that essential and important entities implement appropriate and proportionate technical, operational, and organizational measures. These measures are intended to effectively manage the risks associated with the security of networks and information systems utilized for their operations or the provision of services. Furthermore, the aim is to prevent or mitigate the impact of incidents on the recipients of these services and other related services.

Considering the state-of-the-art and, where applicable, relevant European and international standards and the cost of implementation, the measures shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size, the likelihood of occurrence of incidents, and their severity, including their societal and economic impact.

We have developed "1P360S - MySecurity" solution to address even the most sophisticated security requirements. In accordance with NIS2 Directive, the 1P360S platform and our solutions consistently employ multi-factor authentication or continuous authentication methodologies, as well as military-grade encryption for voice, video, text, and email communications. Additionally, we implement secure emergency communication systems within the organization as appropriate.

# Risk Management Features

## 01. Password Management

Manage and securely store the passwords for all your accounts and external applications in accordance with your organization's Password Policy in a single place.

## 02. E2EE Email Services

Our email system safeguards your communications using advanced quantum-safe encryption and E2EE, providing the highest level of security available in the market today.

## 03. E2EE FileSync Services

Ensure the security and synchronization of your files through E2EE and maintain possession of the encryption keys. No unauthorized parties will have access.

## 04. E2EE Mobile Communications

We utilize one of the most advanced encrypted mobile communication technologies available, the only one in this field that has received NATO certification for military use.

## 05. Virtual Private Network

Our Virtual Private Network (VPN) establishes a secure digital connection between a client device and a remote server operated by the VPN provider. This connection creates a point-to-point tunnel that encrypts data and information.

## 06. Device Management

This function enables the identification, classification, and monitoring of your organization's devices, ensuring that internal and external actions occurring on these devices remain well-regulated and controlled.

# Advanced Measures

## 07. Cloud Backups

Manage automatic cloud security backups for devices connected to your IT infrastructure (e.g. servers, desktops, laptops, mobile devices) to ensure quick recovery when needed.

## 08. EDR Services

Activate Endpoint Detection and Response (EDR), a security solution that continuously monitors your end-user devices to identify and address cyber threats, such as ransomware and malware.

## 09. MDR Services

Implement a Managed Detection and Response (MDR) cybersecurity service that integrates advanced technology with expert human oversight to promptly identify and mitigate threats.

## 10. Patch Management

Patch management is a systematic our procedure involving the identification, acquisition, and deployment of software updates, commonly known as "patches," across a wide array of endpoints

## 11. Access Tracer

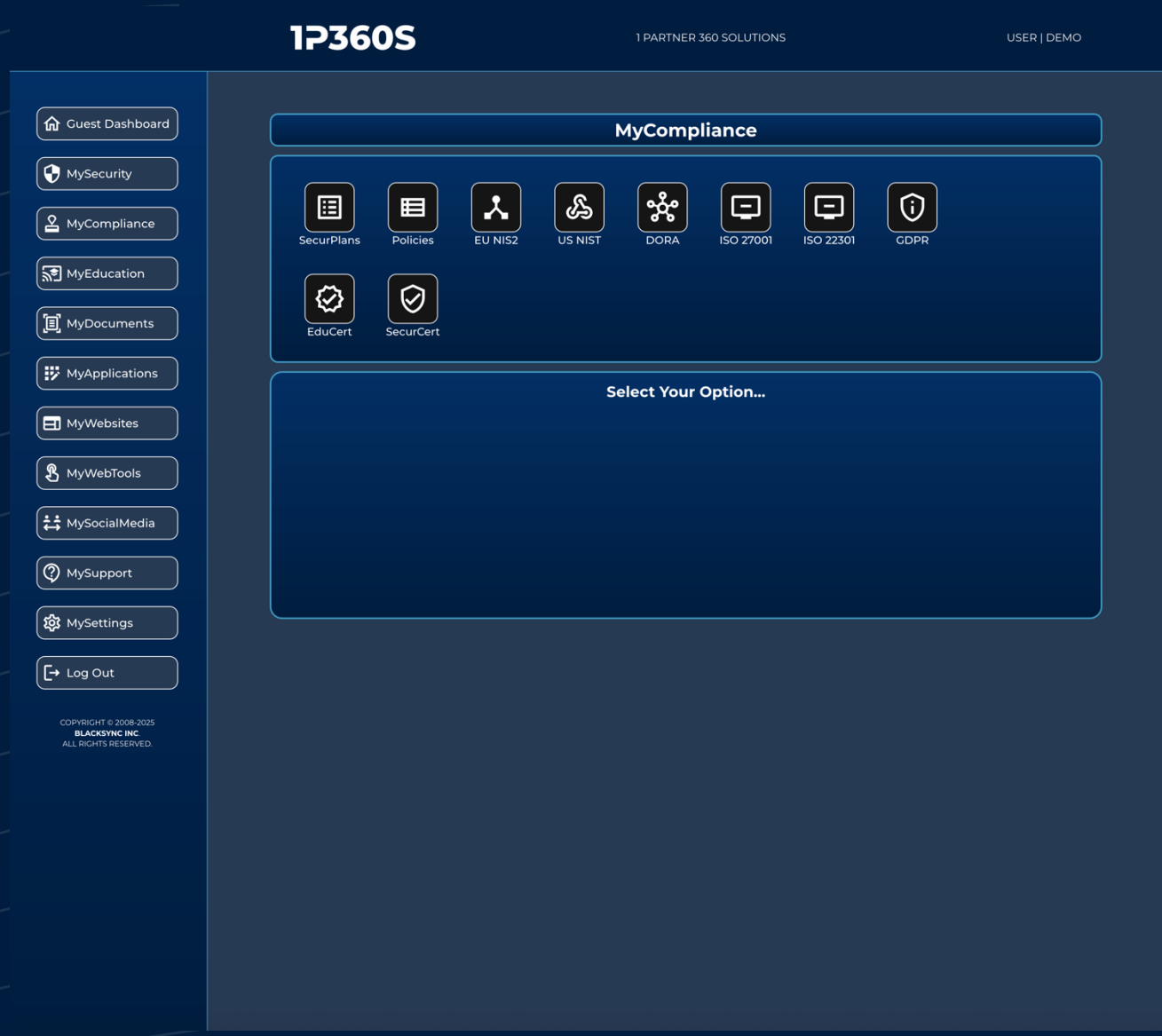
The internal application of 1P360S facilitates the monitoring of user and guest access over an extended period, enabling the verification of all associated activities related to login and logout processes.

## 12. App Tracer

The internal application of 1P360S facilitates the monitoring of all operations conducted by users and guests within the 1P360S platform, even after extended periods.

# Compliance Obligations

Keep your organization compliant



# MyCompliance to respect NIS2 Directive

### Security Plans and Policies

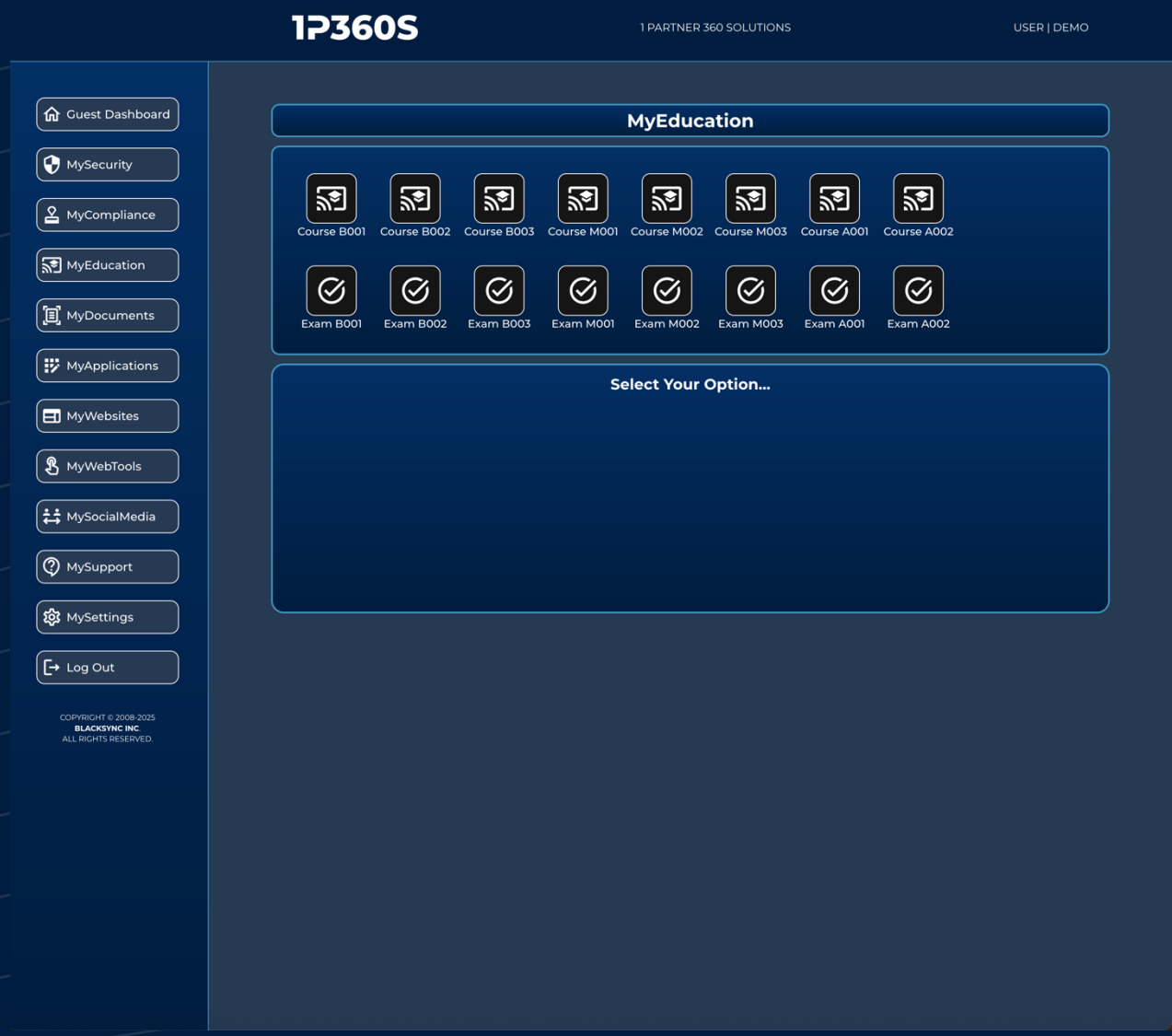
We have developed the "1P360S - MyCompliance" solution to equip our clients with all the necessary procedures and documentation to comply with the NIS2 Directive. This solution encompasses the production and management of multiple security plans, policies, and guidelines, as well as the comprehensive documentation essential for optimizing NIS2 regulatory requirements. All information is generated, modified, and archived automatically, eliminating the need for external Word documents managed manually.

Article 23 of the NIS2 Directive establishes the reporting obligations that every organization must adhere to. Utilizing the security management applications MDR (found in the MySecurity section) and NIS2 application (accessible via MyCompliance), 1P360S is equipped to comply efficiently with the stipulations of the NIS2 Directive. Furthermore, 1P360S can generate all necessary information for mandatory reporting, demonstrating to the relevant national authorities our adherence to security obligations, the management of compliance documentation, and all requirements for timely incident reporting.

In instances where it is necessary to share compliance documentation with external third parties, including authorities, customers, suppliers, and investors, the prospectuses can be produced in a digital format and made accessible to external parties via the Guest Dashboard section, which can be appropriately customized. This approach enhances security and mitigates the risk of losing track of sensitive documents that may otherwise be transmitted via email. In contrast to traditional methods, the 1P360S platform maintains continuous monitoring of document access, recording who accessed the information and the timing of those accesses. This data is retained for an indefinite period, ensuring ongoing oversight and traceability.

# Corporate Accountability

Oversee, approve, and be trained



# MyEducation to manage NIS2 Directive

## NIS2 Directive and Governance

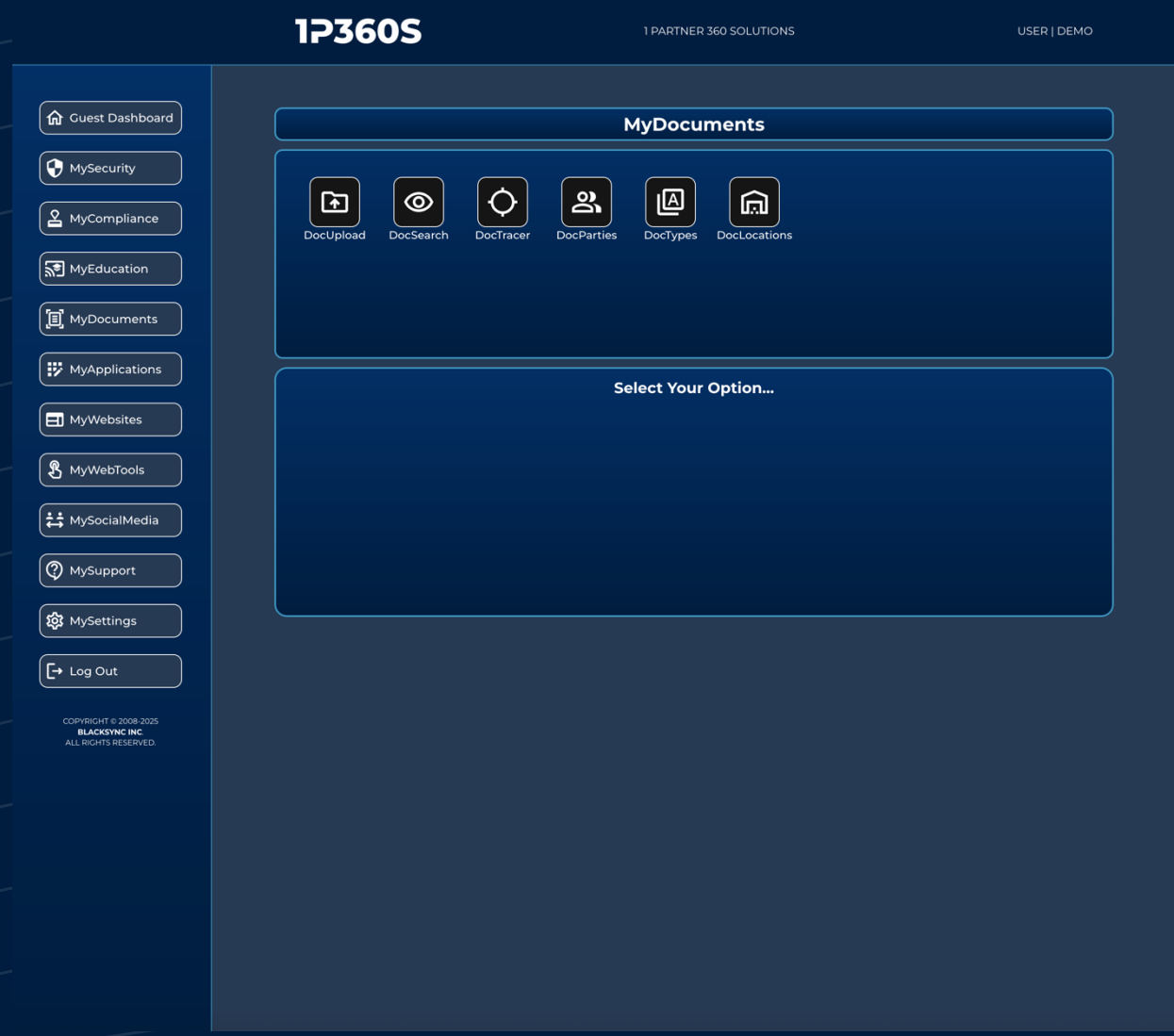
Article 20 of the NIS2 Directive stipulates that Member States must ensure that the management bodies of essential and important entities endorse the cybersecurity risk management measures adopted by these entities to comply with Article 21. Furthermore, these management bodies oversee the implementation of such measures and are liable for any infringements committed by the entities concerning that Article. The application of this provision shall be without prejudice to national legislation about liability rules applicable to public institutions and the liability of public servants and elected or appointed officials.

Member States must ensure that all individuals serving in the management bodies of essential entities are formally mandated to undergo comprehensive training programs. This training must cover critical areas such as risk identification, assessment of cybersecurity threats, and effective risk-management practices. Additionally, Member States shall encourage these entities to regularly extend similar training opportunities to their employees, fostering a cybersecurity awareness culture throughout the organization.

To enhance the security awareness of management and employees within organizations, 1P360S MyEducation Services has developed a comprehensive collection of online courses tailored to three levels of expertise. The basic level provides essential training for office personnel, focusing on fundamental security protocols and practices. The intermediate level is designed for managerial staff, offering in-depth insights into risk management and leadership about security issues. Finally, the advanced level targets IT professionals, exploring complex subjects such as cybersecurity strategies, threat analysis, and advanced technical solutions. Each course aims to equip participants with the knowledge and skills to cultivate a secure work environment.

# Business Continuity

Keep running during times of crisis



# Tools to guarantee business continuity

### BC Plans and DR Plans

To ensure compliance with the requirements set forth by the NIS2 Directive regarding Business Continuity, we utilize the 1P360P platform to prepare and manage Business Continuity Plans and Disaster Recovery Plans for organizations across various sizes and sectors. These plans are mandated by the directive and serve as practical organizational tools that facilitate the efficient management of crises. These plans mitigate costly delays and enhance overall responsiveness by clearly identifying responsible parties and delineating necessary actions.

### E2EE Communication Systems

The most sophisticated attacks on sensitive infrastructures frequently involve malicious actors' proactive monitoring of email and mobile communication systems. Consequently, we have implemented independent end-to-end encrypted (E2EE) email systems and military-grade cellular communication systems within our platform. These solutions guarantee that communications remain secure and cannot be intercepted at any stage before, during, or after an attack. Ensuring the operational integrity and secrecy of communication systems is crucial for effectively managing business continuity as per NIS2 Directive.

### E2EE FileSync application and DMS

The 1P360S platform enhances protection and ensures business continuity by incorporating two independent data backup systems. The first system operates on end-to-end encrypted (E2EE) infrastructure and facilitates the synchronization and distribution of work files, such as Word, Excel, and PowerPoint documents. This capability allows for improved organizational productivity and collaboration with external parties. The second system, named MyDocuments, is responsible for the archiving, management, and accessibility of administrative documents, whether they are scanned paper documents or electronic files. This approach mitigates the risks of transmitting documents via insecure email channels with third parties.

# MyDocuments

## 01. Doc Manager

The application facilitates comprehensive document management capabilities, including the functionalities to upload, search, view, print, and download documents.

## 02. Doc Parties

This table serves as a repository for the components of the document system, specifically the sender and receiver information. It is designed to facilitate the management of documents for DocManager.

## 03. Doc Types

This app serves as a repository for the components of the document system, precisely the type of document. It is designed to facilitate the management of documents for DocManager.

## 04. Doc Locations

App to management the locations where physical documents, which have been digitized and uploaded to DocManager, are stored. This system ensures that the original copies of digital documents can be retrieved efficiently.

## 05. Doc Security

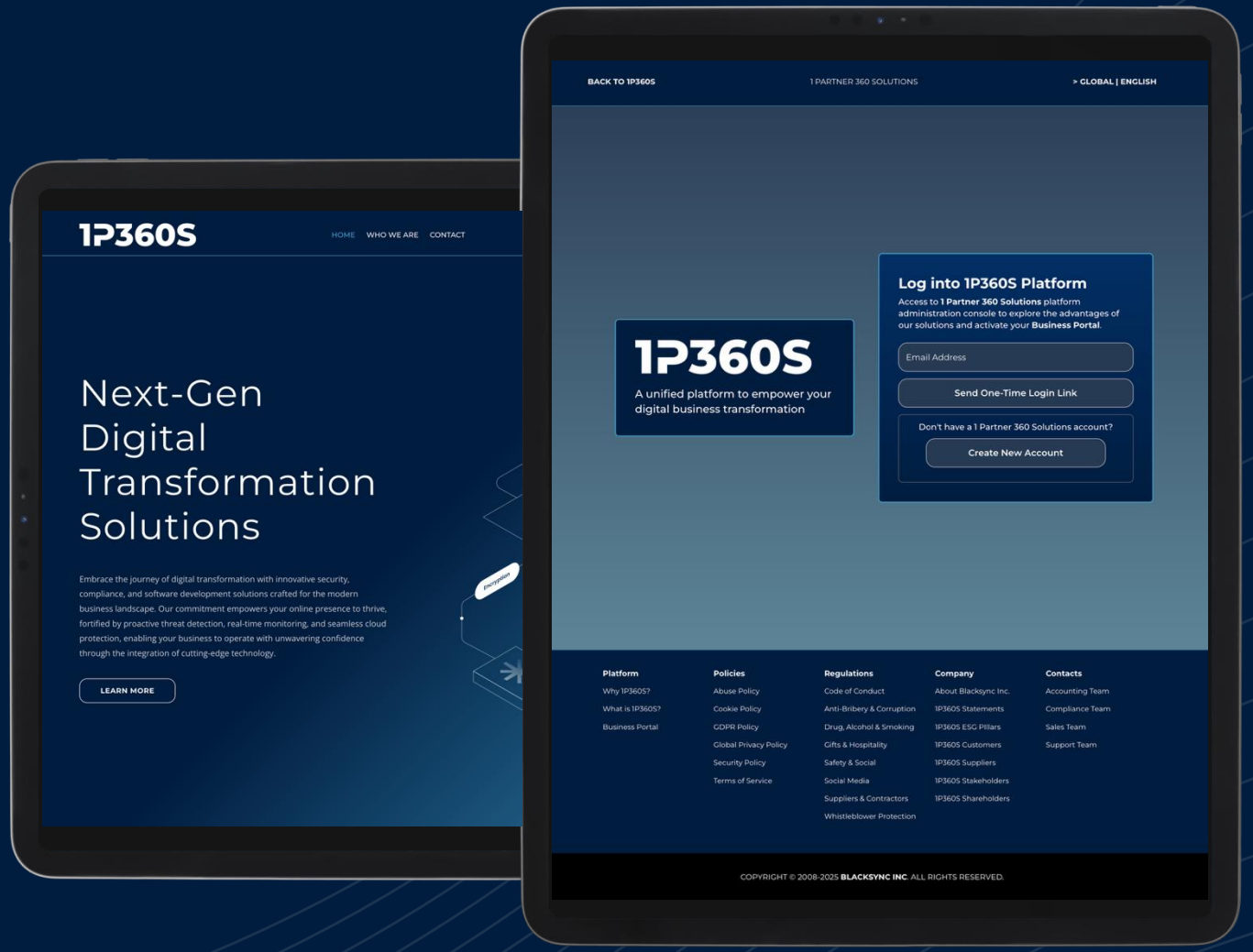
Each uploaded document possesses a designated security level, which ensures that access is restricted to users who have the same or a higher security clearance. This application is designed for managing those security levels effectively.

## 06. Doc Tracer

The application offers a complete security system that lets you monitor user activities. You can see when each user has searched and viewed documents. It also tracks how users engage with each document, showing which users interacted with it and when these activities happened.

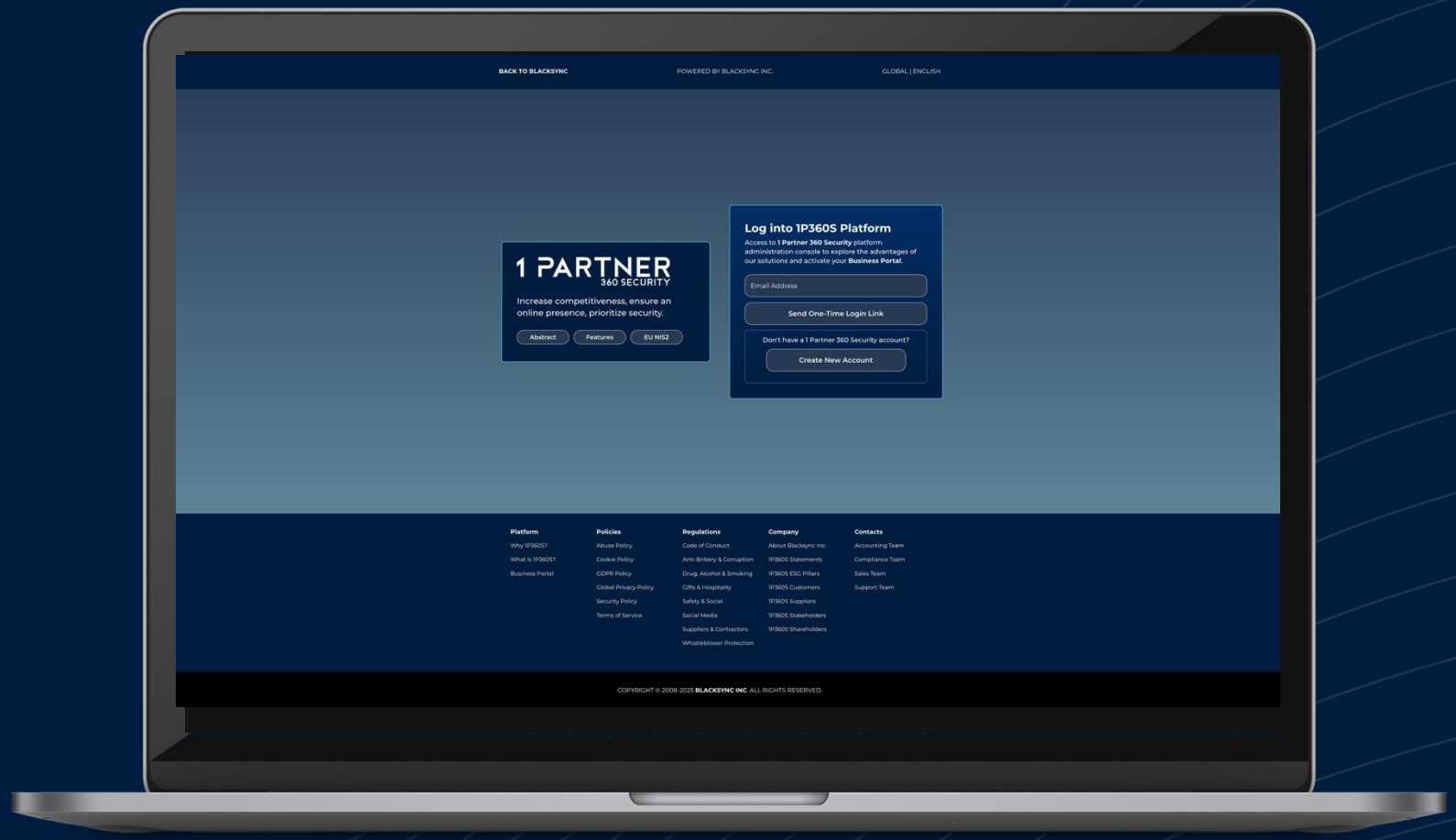
# Your NIS2 Portal Always With You

Utilizing a tablet allows for constant access to your organization's NIS2 Portal, at any time and from any location.



# NIS2 Portal increase your compliance

Utilizing the NIS2 Portal for groups, work teams, and departments significantly enhances an organization’s compliance.



# Thanks!
# **Any questions?**

**You can find us at:**

E: sales@1p360s.com
W: www.1p360s.com