

ПОЛИТИКА

ПО УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА НА „АББ БЪЛГАРИЯ“ ЕООД¹

Системата за управление на сигурността на информацията (СУСИ) като част от Интегрирана система за управление на „АББ България“ ЕООД включва рамка, в която ясно са дефинирани целите и принципите на сигурността на информацията, като едновременно с това създава ясни критерии за анализ и оценка на риска.

СУСИ е съобразена с всички бизнес, правни, технологични, технически и тактически изисквания на процесите по постигане на необходимото ниво на доверие, договорните задължения за осигуряване на сигурността и отговаря на стратегическия контекст за управление на риска в Организацията.

РЪКОВОДСТВОТО, В ЛИЦЕТО НА УПРАВИТЕЛИТЕ:

- Официално декларира настоящата ПОЛИТИКА ПО СИГУРНОСТТА, която е огласена, разпространена, разбрана, прилагана, и поддържана на всички нива в Организацията.
- Официално декларира, че главна цел на Организацията и целия персонал е да създава доверие, като предоставя на своите клиенти, партньори и заинтересовани лица продукт, който да съответства на техните изисквания за сигурност като едновременно с това гарантира конфиденциалност, цялостност и достъпност до информационните активи, осигуряващи процесите на Организацията.
- Поема и носи персоналната отговорност за периодичния преглед и актуализиране на Политиката с оглед на нейната адекватност и непрекъснато усъвършенстване, като този процес се основава само на проверени факти при вземането на решения.
- Има задължението да идентифицира всички процеси по сигурността в Организацията и потвърждава, че те протичат при контролирани условия.
- Ясно определя сигурността на информацията, нейните цели, области и степени на важност, като механизъм за осигуряване и/или използване на информацията. На тази база, Организацията планира ефективни механизми за контрол, които гарантират постигането на поставените цели и се основават на основните принципи на сигурността на информацията.
- Обявява, че основен приоритет за Организацията са идентифицирането на всички рискове за активите, за процесите, продуктите, интересите на клиенти, доставчици, партньори и заинтересовани страни; тяхното анализиране и оценяване; прилагането на ефективни планове за намаляване на риска; изборът и прилагането на подходящи контроли по сигурността, както и оценяването на ефективността от приложените цели и механизми за контрол, като използва това за подобряване сигурността, осигуряване на процес на непрекъснатост на работата и усъвършенстване на Интегрираната система за управление на качеството и сигурността на информацията.
- Непрекъснато изучава и внедрява в Организацията най-новите научно-технически достижения в сферата на сигурността.
- Се стреми да осигури 100% сигурност на всички процеси.
- Осъзнава водещата си роля при формулирането на целите по сигурността и чрез ефикасни механизми за контрол следи за тяхното изпълнение.
- Насочва усилията си в следните направления за ефективното провеждане на ПОЛИТИКАТА ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА:
 - реализиране на ефективни политики по сигурността и създаване на условия за непрекъснато управление на процесите в Организацията.
 - изграждане на модерна система за сигурност на информацията, способна да отговори на високите очаквания на своите клиенти.

¹ Обхват: Централен офис София.

- утвърждаване на Организацията в международен, регионален и национален мащаб по отношение на надеждното и непрекъснато управление на своите процеси и специфични продукти, чрез непрекъснато идентифициране, анализ, оценка и третиране на рисковете за активите, прилагане на адекватни контроли; осигуряване на правно, технологично, техническо и тактическо съответствие и съзнание за сигурност.
- прилагане на специализирани планове за: третиране на риска, непрекъснатост на работата и възстановяване след криза; всестранно осигуряване на сигурността и др.
- ефективно и ефикасно използване наличните иновационни, информационни, материални, човешки и финансови ресурси, съобразно изискванията за сигурност на всички активи.
- управление на непрекъснат процес на обучение, осъзнаване и мотивация на персонала в аспекта на сигурността.

Ръководството осъзнава нуждата да определи План за непрекъснатост на работата на Организацията. Осъзнати са значителните рискове за съществените процеси на работа от потенциални и непредвидени неблагоприятни събития.

За реализиране на тези цели, Ръководството на **„АББ България“ ЕООД** е разработило, внедрило, поддържа и непрекъснато усъвършенства Интегрирана система за управление на качеството и сигурността на информацията, съответстваща на изискванията на EN ISO/IEC 27001:2023, EN ISO/IEC 27001:2023/A1:2024 и другите приложими български и международни стандарти и норми.

КАТО УПРАВИТЕЛИ НА **„АББ България“ ЕООД**, ДЕКЛАРИРАМЕ ЛИЧНОТО СИ УЧАСТИЕ И ОТГОВОРНОСТ ЗА ИЗПЪЛНЕНИЕ НА ОБЯВЕНАТА ПОЛИТИКА ПО СИГУРНОСТТА.

Политиката е дигитално одобрена от Ръководството на Дружеството.

Дата: 01.01.2025 г.

POLICY

ON INFORMATION SECURITY MANAGEMENT SYSTEM

OF „ABB BULGARIA EOOD”¹

The Information Security Management System (ISMS) as part of the ABB Bulgaria EOOD Integrated Management System includes a framework that clearly defines the goals and principles of information security while creating clear criteria for analysis and risk assessment.

ISMS is consistent with all the business, legal, technological, technical and tactical requirements of the processes to achieve the necessary level of trust, contractual obligations to ensure security and meet the strategic context of risk management in the Organization.

THE MANAGEMENT ON BEHALF OF THE GENERAL MANAGER:

- Officially declares this INFORMATION SECURITY POLICY, which is published, distributed, understood, implemented, and maintained at all levels within the Organization.
- Officially declares that the primary purpose of the Organization and all staff is to build trust by providing its customers, partners and stakeholders with a product that meets their security requirements, while ensuring confidentiality, integrity and accessibility of information assets providing the processes of the Organization.
- Accepts and bears the personal responsibility for the periodic review and updating of the Policy with a view to its adequacy and continuous improvement, this process being based only on verified facts in decision making.
- Has the obligation to identify all security processes in the Organization and confirm that they are under controlled conditions.
- Clearly defines the security of information, its goals, areas and levels of importance as a mechanism for providing and / or using the information. On this basis, the Organization plans effective control mechanisms that ensures the achievement of the objectives set and are based on the basic principles of information security.
- Declares that a major priority for the Organization is the identification of all risks to assets, processes, products, interests of customers, suppliers, partners and stakeholders; analysing and evaluating them; the implementation of effective risk reduction plans; the selection and implementation of appropriate security controls, as well as the assessment of the effectiveness of the objectives and control mechanisms applied, using this to improve security, ensure a process of continuity of work and improve the Integrated Quality and Security Management System.
- Continuous study and implementation of the latest scientific and technological developments in the field of security in the Organization.
- It strives to provide 100% security of all processes.
- Is aware of its leading role in formulating security objectives and monitor their implementation through effective control mechanisms.
- Directs its efforts in the following areas for the effective implementation of the INFORMATION SECURITY POLICY:
 - implementation of effective security policies and creation of conditions for continuous management of processes in the Organization.
 - building a modern information security system capable of meeting the high expectations of its customers.
 - promoting the Organization on an international, regional and national scale with regard to the reliable and continuous management of its processes and specific products, through the continuous identification, analysis, evaluation and treatment of asset risks, the implementation of adequate controls; ensuring legal, technological, technical and tactical compliance and security awareness.

¹ Scope: ABB Bulgaria EOOD – Main office Sofia

- implementation of specialized plans for: risk management, continuity of work and recovery from crisis; comprehensive security, etc.
- efficient and effective use of available innovative, information, material, human and financial resources, in accordance with the security requirements of all assets.
- Managing a continuous process of training, awareness, and motivation for security personnel.

Management is aware of the need to establish a Continuity Plan for the Organization. Considerable risks are identified for significant work processes from potential and unforeseen adverse events.

To achieve these goals, **ABB Bulgaria EOOD** has developed, implemented, maintained and continuously upgraded an Integrated System for Information Quality and Security Management in accordance with the requirements of EN ISO/IEC 27001:2023, EN ISO/IEC 27001:2023/A1:2024 and other applicable Bulgarian and international standards and norms.

AS MANAGER OF **ABB BULGARIA EOOD**, I DECLARE MY PERSONAL PARTICIPATION AND RESPONSIBILITY FOR IMPLEMENTATION OF THE PUBLISHED SECURITY POLICY.

The Policy is digitally approved by the Company Management.

January 01, 2025