Polityka Bezpieczeństwa Informacji

Quantifier sp. z o.o.

1. Wprowadzenie

Quantifier sp. z o.o. (dalej: „Quantifier" lub „Organizacja") traktuje bezpieczeństwo informacji jako jeden z fundamentów świadczenia usług swoim Klientom i partnerom biznesowym. Niniejsza polityka przedstawia, w sposób ogólny i przeznaczony do publikacji, zasady funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI, ang. ISMS) wdrożonego w Organizacji.

Quantifier wdrożył System Zarządzania Bezpieczeństwem Informacji (SZBI) zgodny z wymogami normy ISO/IEC 27001:2022. System ten obejmuje zestaw wewnętrznych polityk, procedur oraz mechanizmów nadzoru, których celem jest systematyczna identyfikacja, ocena i ograniczanie ryzyk związanych z bezpieczeństwem informacji.

2. Nasze zobowiązania i cele

W ramach wdrożonego SZBI, Quantifier zobowiązuje się do realizacji następujących celów strategicznych:

- zapewnienia poufności, integralności i dostępności informacji przetwarzanych w związku z działalnością Organizacji oraz świadczonymi usługami,
- zgodności z obowiązującymi przepisami prawa, w tym z przepisami o ochronie danych osobowych oraz wymogami regulacyjnymi i kontraktowymi,
- systematycznej identyfikacji, oceny i ograniczania ryzyk związanych z bezpieczeństwem informacji,
- zapewnienia odpowiedniego poziomu bezpieczeństwa we współpracy z dostawcami i innymi podmiotami trzecimi,
- budowania świadomości i kompetencji w zakresie bezpieczeństwa informacji wśród pracowników i współpracowników,
- zapewnienia gotowości do wykrywania, zgłaszania i obsługi incydentów bezpieczeństwa informacji,
- zapewnienia ciągłości działania kluczowych procesów Organizacji w przypadku zakłóceń,
- ciągłego doskonalenia funkcjonowania SZBI w oparciu o przeglądy, audyty oraz wnioski wynikające z incydentów.

Realizacja powyższych celów podlega okresowemu przeglądowi i ocenie ze strony Najwyższego kierownictwa Organizacji.

3. Zakres systemu

SZBI obejmuje całość działalności Quantifier związanej z przetwarzaniem informacji, w szczególności następujące obszary:

- zarządzanie aktywami informacyjnymi (w tym ich identyfikację, klasyfikację oraz nadzór nad cyklem ich życia, ujęte w Ewidencji Aktywów),
- szacowanie ryzyka i zarządzanie ryzykiem bezpieczeństwa informacji (w tym prowadzenie Rejestru Ryzyka),
- środki bezpieczeństwa technicznego i organizacyjnego oraz zasady kontroli dostępu,
- bezpieczeństwo zasobów ludzkich, w tym szkolenia i budowanie świadomości w zakresie bezpieczeństwa informacji,
- bezpieczeństwo w relacjach z dostawcami i podmiotami trzecimi (bezpieczeństwo łańcucha dostaw),
- zgłaszanie i obsługę incydentów cyberbezpieczeństwa (w tym prowadzenie Rejestru Incydentów),
- zarządzanie kryzysowe w przypadku poważnych incydentów,
- planowanie ciągłości działania i odtwarzania po incydentach.

4. Struktura zarządzania bezpieczeństwem informacji

Za nadzór nad SZBI odpowiada Najwyższe kierownictwo Organizacji (Organ Zarządzający), które zatwierdza polityki, przydziela zasoby oraz okresowo dokonuje przeglądu skuteczności systemu.

W Organizacji wyznaczono Pełnomocnika ds. Cyberbezpieczeństwa (Cybersecurity Officer) odpowiedzialnego za funkcjonowanie SZBI oraz jego Zastępcę, a także inne osoby pełniące funkcje kluczowe dla systemu, w tym osoby odpowiedzialne za zarządzanie aktywami, dostępami, zasobami ludzkimi oraz obsługę incydentów.

5. Zasady ochrony danych przez pracowników i współpracowników

Wszyscy pracownicy oraz współpracownicy Quantifier, posiadający dostęp do informacji lub systemów Organizacji, są zobowiązani do przestrzegania następujących zasad:

- przetwarzania informacji wyłącznie w zakresie niezbędnym do wykonywania powierzonych obowiązków, zgodnie z zasadą minimalnego dostępu (least privilege),
- stosowania bezpiecznych metod uwierzytelniania oraz ochrony danych dostępowych (w tym haseł i innych danych autoryzacyjnych),
- zachowania poufności informacji, do których uzyskali dostęp w związku z wykonywaną pracą lub współpracą, w tym po zakończeniu takiej współpracy,
- niezwłocznego zgłaszania wszelkich podejrzeń naruszenia bezpieczeństwa informacji,
- stosowania zasad bezpiecznej pracy zdalnej oraz korzystania wyłącznie z zatwierdzonych przez Organizację narzędzi i kanałów komunikacji,
- udziału w szkoleniach z zakresu bezpieczeństwa informacji organizowanych przez Quantifier.

6. Wymogi wobec dostawców

Quantifier wymaga od swoich dostawców, podwykonawców oraz innych podmiotów trzecich mających dostęp do informacji lub systemów Organizacji:

- wdrożenia odpowiednich środków bezpieczeństwa informacji, proporcjonalnych do charakteru i zakresu współpracy,
- przestrzegania zasad bezpieczeństwa informacji komunikowanych im przez Organizację,
- niezwłocznego zgłaszania Quantifier wszelkich incydentów bezpieczeństwa, które mogą mieć wpływ na poufność, integralność lub dostępność informacji lub systemów Organizacji,
- współpracy w ramach działań weryfikacyjnych oraz audytowych prowadzonych przez Quantifier, w zakresie uzasadnionym charakterem współpracy.

Niespełnienie powyższych wymogów może skutkować ograniczeniem lub zakończeniem współpracy z danym podmiotem.

7. Zgłaszanie incydentów bezpieczeństwa informacji

Wszelkie potencjalne incydenty bezpieczeństwa informacji dotyczące współpracy z Quantifier, w tym podejrzenia nieautoryzowanego dostępu, utraty danych lub innych zdarzeń mogących wpływać na bezpieczeństwo informacji, należy zgłaszać niezwłocznie na wyznaczony adres:

Kontakt w sprawach bezpieczeństwa informacji: security@quantifier.ai

Każde zgłoszenie jest analizowane i obsługiwane zgodnie z Polityką Zgłaszania i Obsługi Incydentów Cyberbezpieczeństwa oraz pozostałymi wewnętrznymi procedurami Organizacji.

8. Przegląd i aktualizacja polityki

Niniejsza polityka stanowi skrót najważniejszych informacji dla Klientów i partnerów biznesowych wynikających z polityk wewnętrznych składających się na SZBI, przyjętych przez Zarząd Organizacji, i będzie aktualizowana w razie zmian dokonywanych w politykach wewnętrznych, a także w przypadku istotnych zmian w otoczeniu prawnym, regulacyjnym lub organizacyjnym Quantifier.

Information Security Policy

Quantifier sp. z o.o.

1. Introduction

Quantifier sp. z o.o. (hereinafter: “Quantifier” or the “Organization”) treats information security as one of the foundations of the services it provides to its Clients and business partners. This policy presents, in a general form intended for public disclosure, the principles governing the Information Security Management System (ISMS) implemented within the Organization.

Quantifier has implemented an Information Security Management System (ISMS) compliant with the requirements of the ISO/IEC 27001:2022 standard. This system comprises a set of internal policies, procedures, and oversight mechanisms aimed at the systematic identification, assessment, and mitigation of information security risks.

2. Our commitments and objectives

As part of the implemented ISMS, Quantifier commits to pursuing the following strategic objectives:

- ensuring the confidentiality, integrity, and availability of information processed in connection with the Organization's activities and the services it provides,
- complying with applicable laws, including data protection legislation, as well as regulatory and contractual requirements,
- systematically identifying, assessing, and mitigating information security risks,
- ensuring an appropriate level of security in cooperation with suppliers and other third parties,
- building awareness and competence in information security among employees and associates,
- maintaining readiness to detect, report, and handle information security incidents,
- ensuring the continuity of the Organization's key processes in the event of disruptions,
- continually improving the operation of the ISMS based on reviews, audits, and lessons learned from incidents.

The achievement of the above objectives is subject to periodic review and assessment by the Organization's top management.

3. Scope of the system

The ISMS covers the entirety of Quantifier's activities related to the processing of information, in particular the following areas:

- management of information assets, including their identification, classification, and lifecycle oversight (documented in the Asset Log),
- information security risk assessment and management (including maintenance of the Risk Register),

- technical and organizational security measures and access control rules,
- human resources security, including training and awareness-raising in information security,
- security in relationships with suppliers and third parties (supply chain security),
- reporting and handling of cybersecurity incidents (including maintenance of the Incident Register),
- crisis management in the event of serious incidents,
- business continuity planning and post-incident recovery.

4. Information security governance structure

Oversight of the ISMS rests with the Organization's top management (Management Body), which approves policies, allocates resources, and periodically reviews the effectiveness of the system.

The Organization has appointed a Cybersecurity Officer responsible for the operation of the ISMS and their Deputy, as well as other persons performing functions that are key to the system, including those responsible for asset management, access control, human resources, and incident handling.

5. Data protection principles for employees and associates

All Quantifier employees and associates with access to the Organization's information or systems are required to comply with the following principles:

- processing information only to the extent necessary to perform their assigned duties, in accordance with the principle of least privilege,
- using secure authentication methods and protecting access credentials, including passwords and other authentication data,
- maintaining the confidentiality of information accessed in connection with their work or cooperation, including after such cooperation ends,
- promptly reporting any suspected information security breaches,
- applying secure remote working practices and using only tools and communication channels approved by the Organization,
- participating in information security training organized by Quantifier.

6. Requirements for suppliers

Quantifier requires its suppliers, subcontractors, and other third parties with access to the Organization's information or systems to:

- implement appropriate information security measures, proportionate to the nature and scope of the cooperation,
- comply with the information security rules communicated to them by the Organization,

- promptly notify Quantifier of any security incidents that may affect the confidentiality, integrity, or availability of the Organization's information or systems,
- cooperate with verification and audit activities carried out by Quantifier, to the extent justified by the nature of the cooperation.

Failure to meet the above requirements may result in the restriction or termination of cooperation with the relevant party.

7. Reporting information security incidents

Any potential information security incidents related to cooperation with Quantifier - including suspected unauthorized access, data loss, or other events that may affect information security - should be reported promptly to the following dedicated address:

Information security contact: security@quantifier.ai

Each report is reviewed and handled in accordance with the Cybersecurity Incidents Reporting & Handling Policy and the Organization's other internal procedures.

8. Review and update of this policy

This policy constitutes a summary of the key information for Clients and business partners arising from the internal policies comprising the ISMS, adopted by the Organization's Management Board, and will be updated in the event of changes made to the internal policies, as well as in the event of significant changes in Quantifier's legal, regulatory, or organizational environment.