Information Security Framework

We provide our software-in-the-cloud services at safe and sustainable service levels to our customers. We ensure the security of software services end-to-end in an integrated architecture with cloud data centers.

Our security architecture prepared as a result of risk analysis has a certified discipline and life cycle. We operate verification, data protection, monitoring and business continuity methodologies within the scope of our defined processes for compliance with the Law on the Protection of Personal Data (LPPD & GDPR) and other legislation. We periodically overview and renew all our processes for quality assurance.

Security Approach in Cloud Services

The access process of the cloud data centers that we work with to the service and maintenance infrastructures is periodically overviewed by Next4biz. Service providers operate their processes with the methodologies they apply within their own information security lifecycle, and they are monitored by our institution and reported regularly.

The issue we consider the most important in our field of service is to subject all services in the cloud model to global security and compliance regulations and certifications. This approach aims to support the compliance of our customers receiving cloud computing services to global processes.

Cloud data centers carry out independent security tests on their own systems. With the layered and certified architectures in data centers, protection against cyber attacks and natural disasters is obtained at the maximum level in accordance with both ISO and Uptime standards. They are managed by virtualization mechanisms having advanced technology and they provide their reversing processes with independent applications defined in SLAs.

Our service providers have taken the necessary physical measures against natural disasters (fire, flood, earthquake, etc.) and planned attacks (terrorist actions, robbery attempts, etc.).

Our SaaS (Software as a Service) services we provide over cloud services that have Cluster (failover) architecture and TIER III standard, have a shared-firewall infrastructure with CSP support.

Data centers and emergency centers with resilient servers having load-distributing/balancing features are deployed and configured by our service providers. They have a topology providing continuity designed to operate actively and passively in different locations that are not affected by the same natural disaster. They offer redundant “hosting” options with geographical borders that are determined by contract for Cloud Computing services. NTP (Network Time Protocol) can be used and monitored by Next4Biz’s monitoring systems.

Basic Principles of Next4biz Information Security

Governance

“The Information Security, Technology and Guidance Committee” is responsible for the governance and lifecycle of the framework of information systems and information security. The committee plans the necessary controls, measures and monitors defined KPIs and convenes on the agenda every quarter or in shorter interim periods in case of necessity. The committee plans and monitors the company topology, security infrastructure and product development.

The prominent security lifecycles in Next4biz are secure software development, secure access methodology, defined as **SDL** (Secure Development Lifecycle) and control mechanism, defined as **OSA** (Operational Security Assurance).

Information Security Governance

It is of utmost importance to protect the confidentiality of information of our customers. Our main goal is to provide the hardware, software, training, and awareness necessary for minimizing information security risks. To achieve this goal, establishing the required controls and procurement of the resources is our primary principle in governance.

As documented with the certificates we have obtained;

(ISO 27001, ISO27701, ISO22301, ISO 9001, ISO 10002, BS 10012) we aim to ensure the participation of all our employees and business partners in the Information Security Management System (ISMS), which is a holistic approach to information security. For this, together with training and awareness, controlling, monitoring, overviewing and improving the efficiency of ISMS through internal and external audits, are the main stages of our lifecycle.

Next4biz protects the confidentiality, integrity and accessibility of the information and information assets originating from the laws and contracts both its own architecture and our business partners are bonded with and that is processed, stored and managed within the scope and boundaries of their responsibilities.

The risk-oriented approach is aimed at the ISO/IEC 27001 Information security standard. For the protection of information and information assets of organizations in these processes, a correctly planned human resources approach is essential. The level of security aimed by procedures and information technology infrastructures is provided with this discipline in our institution.

The security monitoring architecture is supported by the structure where components are deployed, alarms are monitored (SOC, WAF, internal monitoring, etc.).

Product Development Processes

Our product development processes are defined in sustainable architecture. Processes for analysis, coding and tests are defined and steps necessary for UAT (User Acceptance Tests) and developer unit tests have been established. Change management processes are defined and a disciplinary follow-up approach is executed during software development and in system management architecture.

Penetration tests and source code security and quality analysis and audit procedures are implemented by third-party information security experts.

Applications and interfaces are designed, developed and positioned according to relevant industrial standards (OWASP for web applications).

Quality assurance processes are handled sensitively to increase the level of customer satisfaction. All procedures and transactions are defined.

Access to the System and Segregation of Duties

In accordance with the principle of segregation of duties, authentication matrices are created. Access logs are monitored and authentication rights are reviewed by the Committee described in section 2. All defined procedures and transactions are also overviewed and updated due to relevant and changing circumstances.

Identity, Log Management and Backup Transactions

Application-level verification and system access verification processes are defined and executable. All log records can be monitored and protected.
Backup procedures, recovery transactions, and RTOs (*) are defined.

Governance and Authentication

Our change management, problem-solving and troubleshooting methodologies are in a well-deployed, defined, adopted, and monitored architecture having a high maturity level.

Within the scope of Next4biz activities, personal data processing activities are carried out legally. In this context, as a data supervisor, it is of great importance to protect the personal data of customers, employees, and other natural persons with whom the institution is in relation. The processes of processing and protection of personal data are defined with processes managed by written policies. It is aimed to legitimately process and protect the personal data of our customers, potential customers, employees, employee candidates, visitors, and employees of the institutions we cooperate with.

In this context, Next4biz takes the necessary administrative and technical measures for the processing and protection of personal data under the Personal Data Protection Legislation.

Before granting access to information systems, defined security terms, contract terms, and terms imposed by the governing regulations are regarded.

Standards of access to the databases and authorization are defined and enforceable. All kinds of control and exceptional situations are overviewed and monitored by the defined committees.

Access and Authorization

User passwords are provided according to certain rules. Password length, character repetition, etc. is controlled. In addition, passwords need to be renewed in periods determined by the admin.

Access to the user information database is provided with named users and logged. The user information is stored in an encrypted way. Password attempts without the knowledge of the user and automatic account lockout take place. Notification is made for the password renewals by the admin or the forgotten password transactions performed by the user. Application access is provided by SSL protocol.

Personal Data Protection, Processing, and Retention Policies

In this context, Next4biz takes the necessary administrative and technical measures for processing and protection of personal data under the Personal Data Protection Legislation. Our company has ISO 27701 Personal Data Security certificate.

The processing of personal data with consent and the processing of personal data legitimately and with good faith are covered within Next4biz personal data policies. The need to keep personal data accurate and up-to-date when necessary, and to process the personal data for specific, clear, and legitimate purposes are taken into account. It is essential to process the personal data limitedly, prudently and concerning the purpose of processing, to store the personal data for a period that is projected in the relevant legislation or required for processing, and to illuminate and inform the owners of personal data. Processes in creating the infrastructure necessary for the owners of personal data to use their rights and in taking the necessary precautions for the protection of personal data are defined. In determining and implementing the purposes of personal data processing and transferring the data to third parties, complying with the relevant legislation and PDP

Board regulations and the special regulation of processing and protection of sensitive personal data are included.

Infrastructure, Operational Continuity

Business continuity plans are defined and executed in sustainable architecture. The data for the last 2 years are accessed through production and the data older than 2 years are accessed through the system. The delivery of the records created with the records to the customer in case of termination or cancellation of the contract is provided through the application interface as raw data. In the event of cancellation of the service, all relevant firm, customer and notification data of the firm are deleted from the database. Our company is ISO 22301 certified.

In case of disaster recovery (DR), the RPO value is 12 hours and the RTO value is 8 hours.

(*) RTO Recovery Time Objective
(**) RPO Recovery Point Objective