NxtPort Information Security

Version : 0.1
Date : 30 April 2019

A. *Management Direction for Information Security*

i. NxtPort has implemented an appropriate information security policy.

ii. NxtPort has suitably qualified information security specialists, supported by the NxtPort business leadership.

iii. NxtPort management requires employees and third-party contractors with access to Customer information to commit to written, confidentiality, and privacy responsibilities with respect to that information. These responsibilities survive termination or change of employment or engagement.

B. *Human Resource Security*

i. NxtPort provides information security awareness information to employees and relevant third-party contractors.

ii. Employees are obliged to adhere to regulations on information security, data protection and adequate handling of customer data.

C. *Access Control*

User Access Management

i. NxtPort implements access control policies to support creation, amendment and deletion of user accounts for systems or applications holding or allowing access to Customer information.

ii. NxtPort implements a user account and access provisioning process to assign and revoke access rights to systems and applications.

iii. The use of “generic” or “shared” accounts is prohibited without system controls enabled to track specific user access and prevent shared passwords.

iv. Mandatory strong authentication (two factor authentication) for the CSP's administrators is implemented.

v. NxtPort monitors and restricts access to utilities capable of overriding system or application security controls.

vi. User access to systems and applications storing or allowing access to Customer information is controlled by a secure logon procedure.

Physical Access Management – Facility Security

vii. Physical access to facilities where Customer information is stored or processed is protected in accordance with good industry practices

viii. Policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas

ix. Physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) are implemented.

x. A complete inventory of all critical assets which includes ownership of the asset is maintained.

xi. Two factor authentication for access to the data center is mandatory

xii. Fire protection is available: fire alarm system, fire early detection system, suitable fire extinguishers, regular fire drills.

xiii. Infrastructure is robust and provides adequate resistance to damage by the elements and unauthorized entry

xiv. Redundant data centers that are, at least, far enough away from one another that a controllable damage event does not simultaneously affect the data center originally used and the one containing the backup capabilities

D. Communications Security

Network and Server Security

i. NxtPort logically segregates Customer data within a shared service environment.

ii. NxtPort secures network segments from external entry points where Customer data is accessible.

iii. External network perimeters are hardened and configured to prevent unauthorized traffic.

iv. Inbound and outbound points are protected by firewalls and intrusion detection systems (IDS). c. Ports and protocols are limited to those with specific business purpose.

v. NxtPort synchronizes system clocks on network servers to a universal time source (e.g. UTC) or network time protocol (NTP).

vi. Anti-spam systems are implemented

vii. 0-Day Malware protection is available

viii. Security measures preventing network base attacks are in place

ix. IDP / IDS Systems are implemented

x. Protection against DDoS is implemented

xi. Networks segmentation is implemented.

xii. Direct access from Internet is limited to a separated DMZ.

xiii. Responsibility for the necessary DMZ infrastructure is clearly defined

xiv. Network zones are separated with firewall only allowing necessary network traffic

xv. Application level Firewalls are in place

xvi. Remote administration is done in a secure way

xvii. Remote administration is done via a secure communication channel (e. g. SSH, TLS/SSL, IPSec, VPN)

xviii. Remote login is performed using strong authentication

xix. Network redundancy is implemented

Cryptographic Controls

xx. Customer data, including personal data, is encrypted at rest.

Cloud Controls

xxi. NxtPort encrypts data during transmission between each application tier and between interfacing applications.

E. Application and Data Security

Application Security

i. NxtPort logically segregates Customer data within a shared service environment.

ii. NxtPort secures network segments from external entry points where Customer data is accessible.

F. Operations Security

Service Management

i. NxtPort has implemented formal operating procedures for system processes impacting Customer data. This notification may occur through generic change logs. Procedures must track author, revision date and version number, and must be approved by management.

ii. NxtPort monitors service availability.

Vulnerability Management

iii. NxtPort performs annual penetration testing for systems and applications that store or allow access to Customer data, including personal data. Identified issues must be remediated within a reasonable timeframe.

iv. NxtPort has implemented a patch and vulnerability management process to identify, report and remediate vulnerabilities by:

   a. Implementing vendor patches or fixes.

   b. Developing a remediation plan for critical vulnerabilities.

v. NxtPort has implemented controls to detect and prevent malware, malicious code and unauthorised execution of code. Controls must be updated regularly with the latest technology available (e.g. deploying the latest signatures and definitions).

Logging and Monitoring

vi. NxtPort generates administrator and event logs for systems and applications that store or allow access to Customer data.

vii. NxtPort reviews system logs periodically to identify system failures, faults, or potential security incidents affecting Customer information.

G. Third Party Supplier Management

i. NxtPort has contractual agreements with third parties handling Customer information must include appropriate information security, confidentiality, and data protection requirements, as detailed in the Agreement. Agreements with such parties are reviewed periodically to validate that information security and data protection requirements remain appropriate.

ii. NxtPort reviews its third parties' information security controls periodically and validates that these controls remain appropriate according to the risks represented by the third party's handling of Customer information, taking into account any state-of-the-art technology and the costs of implementation.

iii. NxtPort restricts third party access to Customer data, including personal data.

iv. If requested by Customer, NxtPort provides the Customer a list of third parties with required access to Customer data, including personal data.

v. NxtPort permits access to Customer data, including personal data, only as necessary to perform the services that the third party has contractually agreed to deliver.

vi. NxtPort provides for exit agreements with assured formats and retention of all logical relations and associated costs.

vii. Cloud service providers regularly notifies cloud users about security measures, changes to the IT security management system, security incidents, the results of IS reviews and penetration tests.

viii. Service continuity is monitored with upstream providers in the event of provider failure.

H. Resilience

i. NxtPort performs business continuity risk assessment activities to determine relevant risks, threats, impacts, likelihood, and required controls and procedures. Remediation is conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames.

ii. Based on risk assessment results, NxtPort documents, implements, annually tests and reviews its Business Continuity and Disaster Recovery (BC/DR) plans to validate the ability to restore availability and access to Customer data in a timely manner, in the event of a physical or technical incident that results in loss or corruption of Customer data.

iii. Customer is able, upon request, to monitor measurable parameters as agreed in the SLA.

I. Transparency

i. NxtPort''s locations (country, region) where the customer data will be stored and processed is disclosed and are only within EEA.

ii. NxtPortr's subcontractors who are vital for providing the cloud services are disclosed. Transparency as to which interventions NxtPort or third parties are allowed in the customer's data and processes is given

iii. Regular information about changes is provided (e.g. new or discontinued functions, new subcontractors, other SLA related issues)

iv. Transparency as to which software NxtPort will install onto the customer's systems and the security requirements / risks resulting from this is provided

v. Transparency on governmental intervention or viewing rights, on any legally definable third party rights to view data and on any obligations that NxtPort has to check stored data at any potential location is provided

J. Audit and Compliance

i. NxtPort periodically reviews whether its systems and equipment storing or enabling access to Customer data, including personal data, comply with legal and regulatory requirements and contractual obligations owed to Customer.

ii. NxtPort maintains current independent verification of the effectiveness of its technical and organizational security measures (e.g. ISO certification). The independent information security review are performed at least annually.

iii. NxtPort performs regular independent security reviews.