IBX Business Network Platform

Information Security Controls

2016-11-15 Revision E

Document Classification [Public]

People matter, results count.

Table of Contents

1. General

1.1. There are several objectives of an information security program, but the three main principles of information security are: preservation of availability, integrity, and confidentiality of information and data. These objectives and/or statements are enforced at IBX Business Network by a set of applied control instruments.

2. Physical Security

2.1. **Statement.** Critical or sensitive information processing facilities shall be housed in secure areas protected by defined security measures, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference.

2.2. **Control Instruments.** The IBX infrastructure is hosted in an ISO 9001/27001 certified hosting center in Stockholm, Sweden. While IBX manages hardware and software, the hosting center provides services like electricity, cooling, physical security, shipment etc. these centers provide global enterprises, content companies and network service providers with highly secure, fault-tolerant, redundant, flexible and cost-effective Internet infrastructure solutions.

Only certified and accredited representatives of IBX have access to the IBX infrastructure within the hosting center facilities. The centers adhere to strict security procedures and are equipped with security guards, surveillance cameras and other measures to prevent equipment and data center facilities from being compromised.

3. Network Access Control

3.1. **Statement.** Unauthorized access to IBX infrastructure shall be prevented and user access to both internal and external infrastructure must not compromise the security of the services.

3.2. **Control Instruments.** A monitored firewall separates the IBX corporate network from the IBX production environment. Consequently, unauthorized employees can access data neither from the corporate network nor from the production network. Access is limited to specific employees roles or functions at IBX Business Network. Additionally, access is managed on an "exception" basis whereby personnel need clearance to be authorized. Access is time-limited, after which time re-authentication is required. The access lists are administered by using a dedicated access control product which is integrated with the firewall equipment.

A monitored firewall protects the IBX Business Network reduction network from the Internet. The rules in this firewall are also based on a “deny-all by default” approach: access to systems is explicitly granted with the smallest amount of possible privileges. This solution prevents unauthorized access.

All production networks are monitored for vulnerabilities by using commercial tools.

4. Operating System Access Control

4.1. **Statement.** Unauthorized access to operating system shall be prevented and restricted to only those persons who are authorized to perform system administration/management functions.

4.2. **Control Instruments.** The servers are hardened and accessible only to trained and authenticated technical IBX personnel. Direct access to production servers is limited to technical IBX personnel. All IBX technical staff members with access to production servers are identified on an authorized personnel access list document that is updated whenever staffing changes occur. Accounts are personalized.

5. Application and Information Access Control

5.1. **Statement.** Logical access to application software and information shall be restricted to only authorized users.

5.2. **Control Instruments.** Access to data and functionality at IBX is based on roles and permissions that determine which features of the solution a user can see and work with, and what data a user can access. The set of permissions for a user is derived from the roles attributed to that user and the groups the user may be a member of.

Internet channel security governs communications channel security between IBX applications, IBX office, and other suppliers and buyers. Communication to and from the IBX Business Network occurs over the Internet, so customers' catalogues and transactions must be protected from interception. For increased security, IBX uses HTTP over Secure Socket Layer (HTTPS) for communication by default. The TLS/ SSL protocol is the industry standard method for protecting communications on IP networks. IBX uses TLS/SSL for data encryption and server authentication.

Application security governs end-user's access to the online services and information. The IBX uses unique user IDs and passwords as the primary means of user authentication and access control. All passwords are stored and encrypted in the database.

6. Handling and Processing of Catalogue Information

6.1. **Statement.** Preservation of the integrity and confidentiality of catalogue information provided by the Seller to the Buyer is essential during the handling and processing phase. Data and information submitted by customers may only be handled by authorized personnel and is to be safeguarded by using a combination of technical access control and robust procedures.

6.2. **Control Instruments.** The Seller provides IBX with catalogue data via http(s), SMTP or FTP(s) according to the formats and naming conventions set forth by IBX. The distribution of catalogues to the Buyer follows the process defined by IBX and the Buyer. IBX stores all catalogues data in protected areas that can only be accessed by a limited number of people directly involved with the processing of catalogues. Price information is kept in separate files per Buyer and is only accessed when processing catalogues for a specific Buyer.

Sellers shall provide IBX with price information in separate files per Buyer, according to the formats and naming conventions set forth by IBX. The party from which the information originates is responsible for the correctness of the content of the business documents.

7. Monitoring

7.1. **Statement.** IBX services shall be monitored and information security events should be recorded to detect unauthorized information processing activities. Systems and processes shall also be monitored in order to ensure availability.

7.2. **Control Instruments.** IBX uses centralized monitoring tools to provide maximum alerting capability. It monitors network traffic, processes system messages and alerts, application status, transaction status etc.

IBX uses network based intrusion detection and intrusion prevention. This technology provides logging and alert capabilities to assist in the detection of malicious acts and misuse. It also prevents malicious network traffic and attacks.

To monitor the service levels of the end-user applications, IBX continuously executes pre-recorded scripts to simulate real user behavior to measure real world data from an end-user perspective.

The actual business document flow is monitored with a tool designed to enable the support organization in order to quickly ensure that the business document flow is working correctly and, if not, where the problem is located.

Limited IBX personnel have the rights to access the monitoring systems.

8. Backup

8.1. **Statement.** Data file backup and the ability to recover data is top priority. Accurate and complete records of backup copies and documented restore procedures shall be in place. The frequency of backups should reflect the business and security requirements of the information involved and the criticality of information for continued operation. Backups should be given an appropriate level of physical protection and media should be regularly tested to ensure they can be relied upon.

8.2. **Control Instruments.** Daily backups are performed. These backups do not interrupt the normal operation of the IBX Business Network. Backups are performed by using disk and tape media. Backup tapes are transported to a secure offsite storage location. The backup media is placed in a fireproof safe.

9. Data Protection Act

9.1. **Statement.** The IBX Business Network shall follow local laws regulating data protection.

9.2. **Control Instruments.** The IBX Business Network is hosted in Sweden and follows therefore local law regarding data protection. The Swedish personal data act is based on and implements an EC Directive (95/46/EC) on data protection.

10. Disaster Recovery

10.1. **Statement.** In the case of a severe incident, the effect of the disaster must be mitigated by initiating steps to resume operation in a timely manner.

10.2. **Control Instruments.** IBX has several system recovery plans and business continuity plans that documents the approach and steps for recovering the business. The documents also define roles and responsibilities of the employees in the event of a disaster. Furthermore, the co-location

provider tests power outage backup scenarios on a regular basis in order to ensure the process is up-to-date, successful and effective. IBX offers a recovery time objective (RTO) of 24 hours and recovery point objective (RPO) of 1 hour.

11. Auditing

11.1. **Statement.** The IBX Business Network should regularly be audited for compliance to the ISO 27001 standard and for security vulnerabilities

11.2. **Control Instruments.** The IBX Business Network and its service organization are audited annually to comply with the ISO 27001 certification. The audits are internal as well as external. The IBX Business Network is frequently scanned and security audits are performed by the internal security team following the internal security process for vulnerability management.