bizKonnect

Aggregate, Analyze, Act...

Information Security Policy

Version 5.0

Effective date – January 1, 2016
Last Updated Date – Jan 3, 2021

TABLE OF CONTENTS:

1. INTRODUCTION

GOAL OF THE SECURITY POLICY

Bizkonnect Solutions depends on information and information systems. The goal of the security policy is to set objectives for the organization as regards the protection of its informational assets. The security policy provides the basis for the implementation of security controls that reduce risks and system vulnerabilities. By clarifying the responsibilities of users and the measures they must adopt to protect information and systems, BizKonnect avoids serious losses or unauthorized disclosure. Moreover, the company's good name is also dependant on the manner in which it protects its information and information systems.

SECURITY MANAGEMENT FRAMEWORK

All policies and procedures included in this document are approved, supported and defended by the senior management of BizKonnect Solutions. The security policy is all important to the corporation, its information and the information entrusted to it must be protected according to the critical value and sensitive nature of this information. Security measures must be taken, regardless of the storage media on which information is saved, the systems used to process information or the methods used to transfer information. Information must be protected according to its security classification, without regard to the phase of the information life cycle in which it is found.

SCOPE

The Employees

Information security is a team effort. It requires the participation and support of all members of the organization who work with information systems. Thus, each employee must comply with the requirements of the information security policy and its attending documentation. Employees who deliberately or through negligence violate information security policies will be subject to disciplinary action or dismissal.

The Systems

This policy applies to all computers, networks, applications and operating systems owned or operated by Bizkonnect. The policy covers solely the information handled by computers and networks.

ROLES AND RESPONSIBILITIES

Divisions that manage Information Security

- The Information Security group is responsible for maintaining information security policies, standards, directives and organizational procedures.
- The Internal Quality Division with external consultants must ensure the compliance of information technologies with policies, procedures and any applicable legislation.
- Investigating system hacking and other information security incidents is the responsibility of the System Administration department.
- Disciplinary action in response to violations of information security regulations is the responsibility of local managers acting jointly with the Division of Human Resources.

Responsibility Categories

In order to coordinate security efforts, Bizkonnect has divided the responsibilities of its members into three categories.

a. User Responsibilities

Users are required to conscientiously familiarize themselves with all information security policies, procedures, standards and applicable legislation. They must fully understand these requirements and comply with them.

b. Owner Responsibilities

- Owners of informational assets are generally executives, managers or delegates of BizKonnect who must acquire, develop and maintain operational applications (decision support systems) which support decision-making and other organizational activities.
- Each operational application must have an appointed owner.
- Owners indicate the classification that best reflects the sensitive nature, critical value and availability of each type of information. The classification will, in turn, determine the level of user access.

c. Responsibilities of Information Administrators

- Administrators are staff members who are charged with the safekeeping of company information or information entrusted to the company.
- The personnel of the Information Technologies Division, system administrators and users who handle information on their personal computers all hold the title of administrator.

2. INFORMATION SENSITIVITY AND CLASSIFICATION

FOUR (4) INFORMATION CLASSIFICATIONS

- Information classification constitutes an important element of risk management, as it determines the needs, the priority and the degree of protection required for each type of information.
- BizKonnect has adopted an information classification structure that sees information filed by category. This structure defines the appropriate level of protection for a given category and informs those responsible of any special measures or treatment required.
- All information must be integrated into one of the following four categories.
  - Confidential
  - Private
  - Internal use only
  - Public
- To ensure protection of information, all users must familiarize themselves with the definition of each category as well as the measures required.

INFORMATION LABELLING

- BizKonnect has developed appropriate procedures for labelling and handling information according to the classification structure it has adopted.
- Sensitive information, from inception to destruction, must bear the appropriate information classification designation.
- Identification labels must bear the classification, expiry date of classification, instructions for use and handling, and location, if necessary.
- Labels must appear in the footers of company documents.
- As most documents fall into the "Internal use only" category, it isn’t necessary to put a label on this type of information as it will be classified as such by default.

3. ORGANIZATION SECURITY

DISCLOSURE TO THIRD-PARTIES

- Information labelled other than "Public" must be protected from disclosure to third parties.
- Third-party access to the organization’s information may be permitted if it has been shown that this information is needed to enable the third party to pursue the mandate it has been given by the organization. However, a non-disclosure agreement with Bizkonnect must first be signed and disclosure must be expressly authorized by the information’s owner.
- Any loss or unauthorized or suspected disclosure of sensitive information must be reported immediately to the information owner and to the Information Security Division.

THIRD-PARTY REQUESTS FOR INFORMATION

- Unless an employee has been authorized by an information owner to publicly disclose information, all requests for information concerning BizKonnect must be reported to the management.
- Requests for questionnaires, financial reports, internal policy documents, procedures, surveys and interviews with personnel are covered by this policy.

UNAUTHORIZED COPYING OF INFORMATION

- It is forbidden for users to copy, without valid justification and authorization, the organization’s information or software.
- Those responsible for the unauthorized forwarding of copied information to third parties will be subject to disciplinary action.
- Making backup copies is, however, authorized.

EXTERNAL DISCLOSURE OF SECURITY INFORMATION

Information regarding security measures for information processing systems and networks is confidential and must not be disclosed to unauthorized users, unless first approved by the information security manager. For example, it is strictly prohibited to reveal an employee's home telephone number to a competitor.

4. ADMINISTRATIVE SECURITY CONTROLS

USE OF THE TECHNOLOGICAL RESOURCES OF THE ORGANIZATION

- All employees who wish to use the information processing systems of BizKonnect must sign a compliance statement. In signing this statement, users indicate that they understand and accept to adhere to the policies and procedures of BizKonnect as they relate to the use of computers and networks, including the instructions contained in the present policy.
- The information systems of BizKonnect are to be used solely for professional purposes.

SURVEILLANCE RIGHTS

- Management reserves the right to monitor and inspect the organization's information systems at any time.
- These inspections can take place with or without the consent and presence of the employees involved.
- Information systems likely to be subjected to such inspection include the activity logs of users, hard drive files and email. However, printed documents, desk drawers and storage areas may also be subject to inspection.
- Inspections must only be performed after having obtained the approval of the legal and security departments.
- Management reserves the right to confiscate any offensive material or illegal information.

EXCLUSIVE OWNERSHIP OF DEVELOPED MATERIAL

- Bizkonnect has exclusive rights to patents, copyrights, inventions or any other intellectual property developed by its employees.
- All programs and documents produced or provided by employees for the benefit of BizKonnect are the property of BizKonnect and the latter reserves the right to access and use this information as it sees fit.

INTERNET ACCESS

- All employees of BizKonnect have Internet access at their workstations. This access can be withdrawn at any time, however, at the discretion of management.
- Internet access is monitored to ensure its proper use and compliance with security policies.
- It is forbidden to represent the company on newsgroups or in other public forums unless previously authorized by management.
- Any information received via the Internet should be regarded with suspicion until otherwise confirmed by reliable sources.
- It is forbidden to place company material on publicly accessible information processing systems unless so authorized by the asset owner and the Information Security Division.
- Sensitive information such as passwords and credit card numbers should not be sent via the Internet unless encrypted.

ELECTRONIC MAIL

- BizKonnect provides all employees with an email address and email services in order to facilitate the performance of their tasks.
- All business communications must be sent and received using this email address.
- Personal email accounts (Yahoo, Hotmail) cannot be used for company business unless authorized.
- All personnel must use a standard signature which includes first and last names, position, business address and phone number.
- Important messages should not be stored in the email Inbox.

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

- When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
- These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.
- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

- All servers and computers containing data should be protected by approved security software and a firewall.

DATA BACKUP AND RESTORATION

- Information on individual systems should be regularly backed up on a compact disc or other storage media.
- For multi-user and communications systems, the system administrator is responsible for carrying out periodic backups.
- Backup of the data on laptops is the exclusive responsibility of the laptop user.
- Company data should not be stored on the individual desktops but in respective locations on centralised servers. Individual users will be responsible for the loss or non-availability of data stored on the individual desktops.
- When requested, the Information Technologies Division must provide technical assistance for the installation of backup hardware or software.
- All backup copies of critical or sensitive information must be stored in an approved area with controlled access.
- These copies must be kept solely for the purpose of restoring the system following a computer virus infection, hard drive defects or other computer problems.
- An emergency plan must be developed for all applications that handle critical operational information. The information owner must ensure that the plan is adequately developed, frequently up-dated and periodically reviewed.

DATA USE

- Our own internal data

    - When working with personal and customer data, employees should ensure **the screens of their computers are always locked** when left unattended.

    - Personal employee data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.

    - Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

    - The data should be deleted on request by any employee or any agency. All the data and its source will be tracked and can be referred any point of time.

- External Data in our database used by our clients and some information in that reference
    - All the information we provide is **business** information taken from public sources available to all and given by the individuals to the company or the public sites.

    - We do not collect, process, store or distribute any personal data. We only focus on business data.

    - We remove the person from our database if the person wants the data to be removed.

    - As per our legal review, providing **business** contacts complies with GDPR as long as it is for a legitimate interest like company marketing and as long as it does not violate fundamental rights of an individual.

    - We only collect or action data which is required for our own or our clients' legitimate interests - which according to GDPR Recital 47 includes direct marketing.

      https://www.privacy-regulation.eu/en/recital-47-GDPR.htm

    - As mentioned in this recital - The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

    - The consent from the contacts need to be for a particular purpose when you contact them. Our customers use this information for taking the consent before engaging further in their first communication based on their purpose.

    - We also provide alternate way of connecting with an individual like linkedin URL and integration in addition to the business email id.

  - We do not provide any personal data but you are also permitted to process personal data where you have a “legitimate interest” in doing so that is not overridden by a person’s fundamental rights or interests. In fact, the GDPR states that the “processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.” (This is verbatim from the text of the regulation.)

DATA ACCURACY

The law requires BizKonnect to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort BizKonnect should put into ensuring its accuracy.

- It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer’s details when they call.
- BizKonnect will make it easy for data subjects to update the information BizKonnect holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager’s responsibility to ensure marketing databases are checked against industry suppression files every six months.

CHANGE MANAGEMENT

- Company computers and communications systems used for operational activities must be supported by a documented change management process that ensures only authorized changes are made.
- The change management procedure is applied whenever an important change is made to operations systems, equipment, links or procedures.
- This policy applies to PCs that run operations systems and to larger multi-user systems.

SYSTEM DEVELOPMENT STANDARD

- The development of operational or maintenance software by internal staff must adhere to the policies of the Information Technologies Division and to system development standards, procedures and other conventions.
- These conventions include testing, training and documentation.

MANAGEMENT OF LICENCES

- Management must negotiate appropriate agreements with software suppliers regarding the need for additional licences.
- The supply service will purchase all necessary software. [List of software approved by the supply service is maintained by IT team]

5. ENVIRONMENTAL AND PHYSICAL CONTROLS

ACCESS CONTROL TO INFORMATION AND FACILITIES

- Access to offices, telecommunications rooms, servers and work areas containing sensitive information must be restricted and only granted to employees on a need-to-know basis.
- Sensitive information must always be protected against unauthorized disclosure.
- Hard-copy documents containing sensitive information must be stored in a locked file cabinet.
- Sensitive information must be secured in a locked facility during non-working hours.
- A *clear desk policy* is recommended to further restrict access to documents.
- Computer screens should be positioned so as to reduce the unrestricted view of their contents.

PROTECTION AGAINST THEFT

- System and network equipment must be physically secured with theft-prevention devices when located in an open office.
- Local area network (LAN) servers and other multi-user systems must be placed in locked rooms.
- Portable computers must be protected by key cable locks, placed in locked cabinets or secured by other theft protection devices when located in an unmonitored environment.

6. TECHNICAL SECURITY CONTROLS

USER IDENTIFICATION AND AUTHENTICATION

User ID and password

- BizKonnect requires all employees who access its information systems to have a single user ID and a private password.
- User IDs must be used in order to restrict system access privileges according to the functions, responsibilities and activities of each user.
- All employees are responsible for protecting their user IDs and passwords.

Password Choice

Information system users must choose passwords that are difficult to guess and which contain no information related to their work or personal life. For example, personal ID numbers (PIN, SIN, drivers licence, health insurance number) telephone numbers, names of spouses, postal addresses, proper names, known places or technical terms must not be used.

Here are some tips for creating passwords:

- Think of a word or phrase in your native tongue and spell it in English.
- Combine several words together.
- Combine punctuation or numbers with a word (upper or lower-case letters)
- Transform a common word using a specific method
- Create acronyms (initials forming a word, ex: CEGEP)
- Deliberately misspell a word.

Password Similarity

Users should not repeatedly create passwords that are identical or essentially similar to previous passwords.

Password Constraints

- Passwords must contain at least 8 digits, and be changed at intervals of 90 days or less.
- The password management system obliges users to combine letters and numbers and disallows the repeated use of a password within a given time span.

Password Storage

- Passwords should not be stored in a readable form in sequential files, software macros, computers without access control systems or any other place where unauthorized persons might find them.
- Passwords should at no time be written down and left in plain sight, such on computer monitors or desks, for instance.

Password Sharing

- When information needs to be shared, employees must do so using emails, databases, public directories situated on local area network servers, diskettes, and other exchange media.
- Passwords should never be shared or disclosed.
- System administrators and technical staff should never ask employees to reveal their personal passwords. The only exception is in the case of a temporary password that will be changed when the user accesses the system for the first time.
- If users suspect someone is using their user IDs and passwords, it is their responsibility to immediately advise system administrators.

MALICIOUS SOFTWARE

Virus Detection Software

- System users should not cancel the process of automatic virus definition updates.
- All system files should be scanned by virus detection software.
- A scan must be run before opening new data files and before executing new software.

Elimination of Viruses

- At the first sign of a possible computer virus, employees must immediately cease using the affected system and call technical support.
- All diskettes and other magnetic storage media used on the infected computer should not be used on any other computer until the virus has been successfully removed.
- The infected computer must be quarantined (isolated from the internal network).
- Users must not attempt to delete the viruses themselves.
- Qualified staff members or consultants will remove the viruses and ensure minimal data damage or destruction, and minimal downtime.

NETWORK SECURITY

Internal Network Connection

- All computers that store sensitive information and are permanently or intermittently connected to the organization’s internal computer networks must have an access control system approved by the Information Security Division.
- All other types of information processing systems must be equipped with a screensaver password that locks after a given period of inactivity. The screen is re-activated when the correct password is re-entered.
- Multi-user systems must use a session closing mechanism that automatically shuts down the user session after a given period of inactivity.

External Network Connection

- All external connections to the information systems of BizKonnect must be protected with an approved dynamic password access control system. Dynamic passwords change with each use, rendering their theft useless.
- Employees should not establish connections to external networks (Internet service providers) using the organization’s systems without the prior approval of the Information Security Division.

Network Changes

- Except in emergencies, all changes to the computer networks of BizKonnect must be recorded in a maintenance request and be approved by the Information Technologies Division.
- All changes to internal networks must be carried out by personnel authorized by the Information Technologies Division.
- This process reduces the risk of unauthorized disclosure and of changes being made inadvertently during a moment of distraction without the knowledge of the Information Technologies Division.
- This process applies not only to the employees of BizKonnect but also to service providers.

Teleworking

- Certain employees are authorized, at the discretion of management, to work from home.
- The immediate supervisor of employees wishing to telework must grant permission based on an appropriate checklist.
- Permission to continue teleworking depends partially on compliance with a certain number of policies and information security standards.
- Periodic checking of emails by employees on the road is not regarded as teleworking, but demands respect of the same security regulations.

7. COMPLIANCE

BizKonnect Process Group periodically carries out security audits to ensure compliance with applicable policies, procedures and legislation.

COMPLIANCE WITH POLICIES AND PROCEDURES

All employees must comply with information security policies and related documents. Employees who, by negligence or design, violate security policies will be subject to disciplinary action or dismissal.

COMPLIANCE WITH LEGISLATION AND REGULATIONS

All information security policies must comply with applicable legislation, such as laws regarding data protection, access to information, protection of personal information and electronic documents, etc.

METRICS ON INFORMATION SECURITY

Below are the security Metrics, the implementation of which need to be monitored

1. Percentage of security incidents due to inadequate security policies
2. Percentage of employees who cleared the security check
3. Percentage of employees who signed the NDA
4. Percentage of System users that have received security training
5. Percentage of customers with whom NDA is signed
6. Percentage of vendors/service providers that have not complied with the SLA
7. Percentage of Systems & Service acquisition contracts that include security requirements/security specs
8. Penetration Tests and Vulnerability Assessments, Risk Reassessments performed on schedule and findings closed in time
9. Percentage of users who have visited non-acceptable sites
10. Percentage of security incidents due to non-removal of access rights/non-return of assets for terminated (including resigned) employees

11. Percentage of security incidents caused by improperly configured physical access controls
12. Percentage of planned backups taken as per schedule
13. Percentage of security incidents due to e-mail abuse/non adherence to E-Mail policy
14. Percentage of user accounts not associated with specific users
15. Percentage of security incidents caused by improper passwords/non-adherence to password policy
16. Percentage of equipment behind the firewall
17. Percentage of laptops with encryption enabled

8. DISCIPLINARY MEASURES

- Suspected violations of the security policy (system hacking, virus infections) that could compromise the integrity of information systems must be immediately reported to the Information Security.
- Proven violation or failure to comply with the information security policy entails serious repercussions for offenders. Disciplinary measures vary in accordance to the severity of the violation, and can lead to dismissal.

9. REFERENCES

In order to adequately promote and support information security, BizKonnect has developed policies, procedures, recommendations and standards. These measures, as well as applicable reference legislation, are presented in the following list:

STANDARD REFERENCES

- ISO 17799
- ISO 27001

LEGISLATION REFERENCES

- Personal Information Protection and Electronic Documents Act, Canada
- California's new security breach Disclosure Law (SB 1386)
- Electronic Communications Privacy Act, US
- Information Technology Act, India – 2000
- US Privacy Act
- GDPR, Europe