# ISSP on Network Security Policy for Billingsley-Boscovitch Business Supplies, Inc. (B3SI)

The purpose of this policy document is to ensure the intra-organization technological devices usage and behaviour with them. The new style of saving, and auditing business information will help train and evaluate the employees in future as well as state-of-the art fair use of all network technologies employed by Billingsley-Boscovitch Business Inc. The policy statement defines the roles and scope of employees to engage with the network technologies. The authorized users are defined in organization as employee/people who are working in organization and has log-in information or been provided to use the organizational resources. Any unauthorized login-in to the system will be immediately notified to COO and Manager of IT Grace William and Cecilia Thompson respectively, and they monitor all incoming/outgoing network data/information.

## STATEMENT OF PURPOSE

#### Scope and Applicability

This plan is applicable to all the employees/system managers and/or guest users who use the network and technologies associated with it. The scope defines that all the resources in the network are procession of B3SI organization so a complete authorized usage is mandatory.

#### Definition of Technology Addressed

The range of technologies used in the network of B3SI are given in following section:

* Computers: any machines which is owned by B3SI including desktop, laptop, tablet and server to use and support its network operations.
* Mobile and Cellular Technologies: the technologies which can be connected with server through cellular devices to monitor the network operation
* Personal Digital Assistance (PDA)
* Flash Drives: to carry any documentational/animated information from one place to another which is concerning organizational data
* Storage devices: devices such as CD’s, memory Sticks, Hard Drives and many other removal and portable storage devices
* Email/Internet
* Cloud Database

In longer run all the devices in data centre/server room as well as employer to employee devices also includes in technologies addressed for B3SI installations.

#### Responsibilities

For the fair use of resources owned by B3SI the roles and responsibilities of each employee and staff is different so are their authority with the system. Staff and employees according to their responsibilities are defined for authorization of role in the organization. The major hierarchy of responsibilities includes:

1. Receptionist: can use the network to fix the meeting timings, availability and management of different meetings in the meeting room, coordinate the time between vendors and management, management to employees etc.
2. Executive assistant: can use the system fairly to evaluate the overall sales, reporting, and generating the data to be presented as overall sales and purchase reporting.
3. CEO: can view and administrate all the information of the organization and have full access and view of the network system.
4. COO: have information and view of system but can’t edit or update all parts of the system without proper authorization
5. CFO: have information and view of system but can’t edit or update all parts of system without proper authorization
6. Purchasing Rep: have authorization and responsibility to maintain the purchasing information, vendors information and add information to the ledger. The traverse distribution software defines the role for purchasing rep.
7. Manager Purchasing: he can edit, view, and update all the purchasing information in ledger and can send billing to the vendors and managers through reporting.
8. Purchasing Admin Assistant: he can view, edit and update the purchasing information and generate reporting for the higher management
9. HR Admin Assistant: he can get the employees information through HRIS system for payroll management, human resources management and time and attendance management.
10. Manager, HR: he can view, and update and report the HRIS system for payroll and human resources management.
11. Sales Rep: in Traverse Accounting software the user role for sales rep is to get the sales for the B3SI and they can enter the sales they made in a day to the system
12. Manager, Sales: the manager can view and update the sales on the daily basis and generate report for each station of sales
13. Sales Admin Assistant: he can view the reporting of sales from each sales point and generate a report accordingly to send to distribution management to fulfil the demands of each station.
14. Distribution Rep: in Traverse distribution software they are given the role to fulfil as distribution rep for each station
15. Manager, Distribution: he can view and manage all the distribution of good for all sales stations
16. Accountant, General Ledger: traverse account software will define his role to use the network to maintain the general ledger and view all the banking, and information related to monetary value of the organization
17. Manager, IT: he can use Traverse ERP system to view and update and manage all the information for the web portals and customer relationship management.

## Authorized Users

#### User Access

The user access can be distributed to four major roles to be defined:

1. Accounting: the users who are related to bank, ledger maintenance and accounting management like accountants, accounting manager will be given the authorized use of accounting software
2. Traverse distribution software user access: the sales, purchase and distribution management and reps will be authorized this software access according to their role in the system
3. Traverse ERP: this system will be used by IT personnel to maintain the system information as well as the CRP system
4. HRIS system: the users related to human resources management will be assigned to this system according to their roles.

#### Fair and Responsible Use

All the four majorly defined user access points are managed by the management teams which will ensure the fair and responsible use of system by the system admins, accounting admins, distribution software admins and ERP Admins and HRIS admins. All the admins of the different systems in the network will be responsible to conduct the fair use of the system.

#### Protection of Privacy

For the user’s protection of privacy all the users who are using the system will be given special names by the system which will protect their privacy. The other protection provided by the network will be to ensure that no outside attack can be made through strong firewall installation. the users will be given protection.

Only authorized people will be accessing the information of their sub-ordinates to confirm their performance over the system and given authorization will be through their consent.

## Prohibited Uses

#### Disruptive Use or Misuse

Any use of the system which don’t directly support the B3SI use of its four major Systems on the network, is considered misuse and thus is expressively prohibited. This may includes but not limited to social media websites, shopping websites, entertainment sites etc. except they are related to official business.

All users of the system are prohibited to use the B3SI resources assigned for network use or outside business hours or from outside the organization are considered as disruptive use of misuse of the system

All users of the system are prohibited to use their personal devices to connect to the network for their personal use as this will be a disruptive use of organizational resources

#### Criminal Use

B3SI will adopt a strict policy for any sort of criminal activity being performed on the network data, and anyone hold with such irresponsible behaviour will be hold prosecution for illegal use of resources.

All users of the B3SI network information security are prohibited from the use of network in illegal, illicit or criminal activities.

Any unauthorized attempt to gain the B3SI network authorization will be considered as criminal use and will be prosecuted.

#### Offensive and harassing Material

B3SI promotes and support a work environment with free from harassment or exposure to the offensive materials. Any use of B3SI network information for such purpose to create hostile work environment will be investigated by third organization for human rights and will face national work harassment laws and face court for harassment actions. The organizational misconduct will be handled internally and separately.

#### Copyrights, licensed or intellectual property misuse

According to US copyright law, as well as laws and regulations for the US employment and employer law the IP for this network security is license and any misuse will be considered a criminal and license properly misuse conduct and will be treated accordingly to copyright law of the US.

## System Management

#### Management of Stored Material

The stored office material all the warehouse, network information to include but not limited to as both hardware, electronic and information associated with network security is responsibility of respective department and employees to protect and should fulfil their own responsibilities in the system.

#### Employer monitoring

B3SI reserves the right to monitor its employees communication between seller and vendors, and customers regarding to data transmittal, storage and information processing by using the network for information security and any suspected violation of its policy, criminal actions and information security breach, malware installation or any other activity will be considered a offense.

#### Virus protection

B3SI is motivated to protect its system by installing proper firewalls to protect its system from outside attack but at the same time urges its employees to follow the organizational policy and don’t install such programs or things which can cause installation of malware or viruses which can cause system harm and delay of system delivery for vendors and customers.

#### Physical Security

B3SI have taken all the parameter and measurements to protect its assets physically and have properly installed security. The admin and regulation provides the physical security.

#### Encryption

B3SI have installed the encryption software to provide security to the network information, but at the same time the encryption policy is updated time to time for successful communication.

## Violation of Policy

#### Procedure for reporting Violations

Anyone who is observed a violation of this policy statement should be immediately reported to the B3SI office of policy-violation-and-reporting using the anonymous web forms at organization web portal.

#### Penalties for Violation

According to offense the organization will take steps towards the penalties up-to termination depending upon the value of violation of policy terms of this document

## Policy Management

#### Schedule a Review Policy

For any unexpected or new event which can lead to develop new review policy can always be considered depending upon case, situation or national law for occupation and labour laws and security laws.

#### Procedure of Modification

The revised policy will be circulated inside the organization for comment over a period of 30 days following a review cycle. The review recommendations, improvement and submissions will be discussed, and modifications are developed accordingly.

## Limitations of Liabilities

#### Statement of Liability

B3SI will not tolerate and accept any liabilities associated with the conduct of any individual violating the policy and in doing so is committing a crime.

In addition, B3SI will assist in prosecution of any individual who does so, so long as schedule legal actions in best interest of B3SI.