

# Information Security Policy

## 1.0 PURPOSE

This policy establishes information security requirements to ensure that company information, which is considered an asset, and technologies are not compromised, B Bowden and company is committed to ensuring the highest level of client Data security.

## 2.0 SCOPE

In recognition of the critical role that information systems play in B Bowden and Company business activities, this policy defines the rules and requirements necessary for the secure and reliable operation of the B Bowden and Company information systems infrastructure. This policy applies to all B Bowden and Company employees and third parties who access B Bowden and Company systems.

## 3.0 POLICY

Every individual at B Bowden has information security roles and duties. For example, it is every individual's duty to report information security incidents. Similarly, system designers at Oliis Design (B Bowden and Company IT Designers) are required to include necessary security measures into systems such as restricting user access based on the user's need-to-know.

### *3.1 Ownership, Administration, and User-Responsibilities*

B Bowden and Company Information may include information owned by B Bowden and Company, its customers, its shareholders or its employees. All users of B Bowden and company Information have special responsibilities related to security and compliance, which are described in this policy. If you are not sure which of the following roles are applicable to you, ask your manager for guidance.

3.1.1. Company Directors – must be identified as part of the design process for all systems at B Bowden and Company. They are responsible for; rather they are empowered by B. Bowden & Company to make the following decisions regarding this information:

- \* Approve information-oriented access control privileges for specific job profiles.
- \* Approve information-oriented access controls requests that fall outside existing job profiles.
- \* Designate a master data source for information from which management reports will be derived.
- \* Establish internal controls needed to ensure data integrity as appropriate (such as input validation checks and backup procedures).
- \* Define acceptable limits on the quality of their information (accuracy, timeliness, etc.)
- \* Approve all new and different uses of their information and be aware of current uses of their information.
- \* Approve the use of their information in all new or substantially enhanced application systems before these systems are moved into production operation status.
- \* Periodically review reports that indicate the job profiles, personnel or transaction codes that access their information to ensure appropriateness.
- \* Select and periodically review a criticality category relevant to their information so that appropriate contingency planning can be performed.

Company Directors must be full time employees of B Bowden and Company and must designate a backup to act if they are absent or unavailable. Directors may not delegate ownership responsibilities to third party organizations or to any individual who is not a full time B Bowden and Company employee.

3.1.2. Information Custodians (Management and Supervisors) – are the people with physical or logical control of information, such as (for example) systems administrators and database administrators. In some cases, when information is portable (USB Storage, paper, CD, Laptop Hard Disk, etc) the Information User has the responsibility of the Information Custodian as well. In most cases, the selection of Information Custodians will be based on existing operational procedures. If this is not the case, the Directors will appoint an Information Custodian. Information Custodians implement and operate systems acting on behalf of Company Directors

and provide Directors with technical information and consulting needed for them to make decisions regarding the security of their information. Information Custodians also provide services to Information Users specified by the Directors.

Information Custodians must preserve information in their custody against loss, unauthorized disclosure and corruption; must not send information to parties other than those authorized; must not change information in their care without authorization; and must not be Information Users of the information in their custody.

3.1.3. Information Users – access to B Bowden and Company owned or controlled information is dependent on each user's job profile. When an Information User needs access to a new set of B Bowden and Company owned or controlled information, this request is subject to the approval of their immediate manager and the responsible Information Trustee or their designee. An Information User's access to B Bowden and Company owned or controlled information must be terminated when the relationship between B Bowden and Company and the User ceases or when the Information User's role changes such that such access is no longer necessary for the Information User to perform his or her job.

### *3.2 Incident Detection*

Individuals are required to immediately report any suspected or confirmed breach of information security at B Bowden and Company or any known or suspected threats via the Financial Director.

3.2.1 Any B Bowden and Company employee who witnesses or is involved in a computer security incident should gather as much information as possible under the circumstances. Employees should attempt to collect information such as: name or names of affected assets, process that was affected, time and date of incident (or best knowledge of), etc. Employees unsure of what to do when faced with a computer security incident should immediately contact the Financial Director for guidance.

3.2.2 Information on affected systems may be collected as evidence. Information may not be modified in any way. If it is not clear how to preserve evidence or what course of action to take, please refer to the Financial Director.

3.2.3 Once the Employee gathers the appropriate information, the Employee should both open up an issue with the Financial Director.

### *3.3 General Configuration Requirements*

Since many attacks and viruses prey upon improperly patched or configured systems it is imperative that every computer connected to the B Bowden and Company network is properly secured and that all software and hardware conform to B Bowden and Company Computer Usage Policy.

3.3.1. All network activity between untrusted networks (including the Internet and wireless) traffic and within the B Bowden and Company network must go through a managed firewall or access control list.

3.3.2. Original firewall configurations and any changes thereto must be reviewed and approved by Evolution IT, who may require security improvements as needed.

3.3.3. Port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the network are prohibited.

3.3.4. Traffic between production networks and R&D networks, as well as traffic between separate R&D networks, is permitted based on business needs and as long as the traffic does not negatively impact other networks. R&D must not run network services that may compromise production network services or put R&D confidential information at risk.

3.3.5 In instances where non B Bowden and Company personnel (who are not under NDA) have physical access to R&D environments, direct connectivity to the corporate production network is not allowed. Additionally, no B Bowden and Company confidential information can reside on any computer equipment at unspecified locations. Connectivity for authorized personnel from these locations can be allowed to the production network only if authenticated against the Evolution

Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by Evolution IT.

#### *3.4 Anti-Virus Requirements*

3.4.1 All software media being supplied to external entities or for distribution within B Bowden and Company must be scanned for viruses.

3.4.2 It is prohibited to introduce mal-ware, Trojan horses, worms, portable infections and infectors, or other viruses to any B Bowden and Company systems or networks. Oliis Design and Evolution IT are the only B Bowden and Company personnel excluded from this policy due to the nature of their work- however they must comply with all appropriate procedures and use proper safeguards.

3.4.3 Infected systems may not, under any circumstance, be connected to the B Bowden and Company network. Once an infection has been identified, the affected system must be disconnected from the B Bowden and Company network and properly remediated (including the removal of any secondary back-door application or configurations). After it has been remediated it must then be properly secured as per Evolution IT configuration and patch checklists, before it can be reconnected to the B Bowden and Company network.

#### 3.5 Host Security

3.5.1 All hosts must be configured securely. Open file shares and weak passwords are examples of unacceptable configurations that can lead to a system compromise.

3.5.2 Systems must be patched to current standards in accordance with Evolution Guidelines.

3.5.3 Systems that are not maintained by Evolution are the responsibility of the system owner to ensure patch, configuration, administration and anti-virus compliance.

Any employee found to have violated this policy will be subject to disciplinary action, up to and including termination of employment.

### **4.0 DEFINITIONS**

- External Connections - External connections include (but not limited to) third-party data network-to-network, analog and ISDN data lines, or any other Telco data lines.
- Lab Owned Gateway Device - A lab owned gateway device is the device that connects the B Bowden and Company training network to the rest of Bowden and Company network. All traffic between the lab and the network must pass through the lab owned gateway device unless approved by Evolution.
- Telco - A Telco is equivalent to a service provider. Telcos offer network connectivity, e.g., T1, T3, OC3, OC12 or DSL. Telcos are sometimes referred to as "baby bells", although Sprint and AT&T are also considered Telcos. Telco interfaces include Basic Rate Interface (BRI) - a structure commonly used for ISDN service, and Primary Rate Interface (PRI) - a structure for voice/dial-up service.
- Firewall - A device that controls access between networks. It can be a PIX, a router with access control lists or similar security devices approved by Evolution IT.
- Extranet - Connections between third parties that require access connections to non-public B Bowden and Company resources.

### **5.0 KEY DOCUMENTS AND SYSTEMS**

None.

### **6.0 ROLES AND RESPONSIBILITIES**

- Information Trustees (Company Directors) – Individuals or Groups that manage information on behalf of the owner, B Bowden and Company or its partners, customers, or

shareholders. Information Trustees may, in some cases, not be permitted to be Information Custodians, if there would be an unacceptable Segregation of Duties.

- Information Custodians – Administrative controls for security, confidentiality, and/or integrity of data by following the requirements set forth by Information Trustees. Information Users who possess B Bowden and Company Information in a portable form are also Information Custodians.
- Information Users – Individuals or groups that transport, transform, or use B Bowden and Company managed information.
- Evolution IT and Ollis Design- The team within B Bowden and Company IT Service Organization, responsible for security strategy and standards.

## **PROCEDURES**

A designated employee agreed with the Financial Director can only process data and information received by Contract Originators.

It is the Financial Director's responsibility to vet information and Data and decide the process of the information to be entered on Backstage, also to assign the appropriate member of staff that will be the accounts co-coordinator for that contract.

Once a specific procedure has been set up for each individual contract, the Financial Director will assess the procedure quarterly referring to report figures run by Backstage IT System and the Clear Desk Policy.