BBE TRAINING | A CITRUS GROUP COMPANY

Security Policy for BBE Training

Security Policy Statement

BBE Training Ltd
Service units within the centre are charged with the primary responsibility and authority to ensure that BBE Training Ltd meets external and internal requirements for privacy and security of specific types of confidential and business information (e.g., student educational records, personnel records, health records, financial transaction data). These units are responsible for other general security issues and for assisting in the development of the centres IT security policies, standards and best practices in the areas of their responsibility. They are also responsible for advising centre, departments, and individuals in security practices relating to these areas:

- Financial information and transactions
- Health information
- Infrastructure, communications, and systems security
- Legal issues
- Library circulation records
- Personnel information and confidentiality
- Physical building security
- Research information, confidentiality, and compliance
- Security audits
- Student loan information
- Student record information and confidentiality

Centre, Departments, and Other Units

Centre, departments, and other units are responsible for securing any information they create, manage, or store, and for any information they acquire or access from other party systems (e.g., student educational records, personnel records, business information). This responsibility includes completing periodic risk assessments, developing and implementing appropriate security practices, and complying with all aspects of this policy.

Third Party Vendors

Third party vendors providing hosted services, sometimes referred to as Application Service Providers, and vendors providing support, whether at our centre or from a remote location, are subject to BBE Training ltd security policies and will be required to acknowledge this in the contractual agreements. The vendors are subject to the same auditing and risk assessment requirements as the centre, departments, and other units. All contracts, audits and risk assessments involving third party vendors will be reviewed and approved by the centre based on their area of responsibility.

Individual IT System Users

Every member of the centre community is responsible for protecting the security of BBE Training information and information systems by adhering to the objectives and requirements stated within published centre policies. In addition, individuals are required to comply with the additional security policies, procedures, and practices established by the centre and other colleges, departments or units. Failure to comply with established policies and practices may result in loss of computing privileges and/or disciplinary action.

Security Policy for BBE

Students, faculty, and staff who use personally-owned systems to access centre resources are responsible for the security of their personally-owned computers or other network devices and are subject to the following:

- The provisions of the IT Security policy and the standards, procedures, and guidelines established by BBE Training ltd computing and network facilities.
- All other laws, regulations, or policies directed at the individual user.

Other Registered Entities

Any entity that is a registered user and connected to the centre network is responsible for the security of its computers and network devices and is subject to the following:

- The provisions of the IT Security policy and the standards, procedures, and guidelines established by BBE Training ltd computing and network facilities.
- All other laws, regulations, or policies directed at the organisation and its individual users.

Reporting of Security Incidents (All Users)

Reporting security breaches or other security-related incidents is an ethical responsibility of all members of the centre and BBE Training ltd. A critical component of security is to address security breaches promptly and with the appropriate level of action. The IT Security Incident Reporting Policy outlines the responsibilities of the centre, departments, units, and individuals in reporting as well as defining procedures for handling security incidents.

Risk Assessment

The purpose of risk assessment is to help ensure that threats and vulnerabilities are identified, the greatest risks are considered, and appropriate decisions are made regarding the risks to assume and those to mitigate through security controls. Risk assessments will be conducted at various levels as found under Security Roles and Responsibilities.

The following key factors will guide the process to insure a successful risk assessment program:

- A centre department or unit will be designated as responsible for conducting a risk assessment and at a prescribed frequency in the Schedule of Risk Assessments for Information Security.
- Risk assessments will involve both the administrative department responsible for the business operation and the technical staff supporting the systems.
- Final sign-off by the department head of the organisation doing the risk assessment indicating agreement with risk acceptance and risk reduction decisions.
- Documentation of risk assessments and resulting actions will be placed on file for audit and accountability purposes.

Education

All units-from the centre, department, and unit level-must provide opportunities for individuals to learn about their roles in creating a secure IT environment. Creating a heightened awareness of the importance of information technology security is an important component in establishing an environment in which each individual feels both responsible and empowered to act in their own and the community's best interests.

Systems

BBE Training Ltd use a secure exchange email system backed up to a Linex secure server. This server has a secure bunker bank up system based away from the main centre site.

No sensitive date or files will be stored directly on any local computer. All files are encrypted and backed up with 7 days of backup storage every evening. External backups are created daily with drives securely stored in overnight safes away from centre.

Last review: June 2023

Next review: June 2024