Third-Party Supplier / Vendor Code of Conduct (Policy)

Purpose

The purpose of this Policy is to establish requirements for ensuring third-party service providers/vendors meet BASIC’s requirements for preserving our information and protecting it against misuse, compromise or loss, as well as build around our belief that everything will be measured against the highest standards of ethical business conduct.

Scope

This Policy applies to all third-party suppliers /vendors (and Partners) of Belcasoft International Corp. (“BASIC”, or “We”), who have the ability to impact the confidentiality, integrity, and availability of RigER Products and sensitive information, or who are within the scope of BASIC’s Information Security Program.

Who must follow the Policy?

We expect all third-party suppliers / vendors to follow the Policy. Failure to do so can result in termination of the relationship with BASIC.

Code of Conduct

BASIC makes every effort to assure that all third-party organizations (including cloud service providers) are compliant and do not compromise the integrity, security, and privacy of BASIC.

As a BASIC supplier/vendor you’re expected to act ethically and demonstrate integrity in all situations. You have a duty to follow policies and procedures found in this Code of Conduct, as well as those that are specific to your contract. You must also comply with all laws that apply to our business.

Quality Work Environment

We are committed to a supportive work environment, where our personnel have the opportunity to reach their full potential. Members of BASIC team, as well as all third-party suppliers/vendors are expected to do their utmost to keep the workplace culture free of harassment, intimidation, bias, and unlawful discrimination.

Equal Opportunity Employment

We strictly prohibit unlawful discrimination or harassment on the basis of race, color, religion, veteran status, national origin, ancestry, pregnancy status, sex, gender identity or expression, age, marital status, mental or physical disability, medical condition, sexual orientation, or any other characteristics protected by law.

Drugs and Alcohol

Substance abuse is incompatible with the health and safety standards that BASIC adheres to, and it's not permitted. Consumption of alcohol is allowed at our office on special occasions, but we ask everyone to use good judgment and never drink in a way that: (i) leads to impaired performance or inappropriate behavior, (ii) endangers the safety of others, or (iii) violates the law. Illegal drugs are strictly prohibited in our offices or at work-related events.

Safe Workplace

We are committed to a violence-free work environment. We will not tolerate any level of violence or the threat of violence in the workplace.

Obey the Law

BASIC takes its responsibilities to comply with laws very seriously. Every third-party supplier/vendor is expected to comply with applicable legal requirements and restrictions. You should understand the laws and regulations that apply to your work during the engagement with BASIC.

Confidentiality/Non-Disclosure Agreement (NDA)

BASIC uses non-disclosure agreements to protect confidential information using legally enforceable terms. NDAs are applicable to both internal and external parties. NDAs will have the following elements:

- Definition of the information to be protected
- Duration of the agreement
- Responsibilities and actions to avoid unauthorized disclosure
- Ownership of information, trade secrets and intellectual property
- Permitted use of the confidential information and rights to use information
- Process of notification and reporting of unauthorized disclosure or information leakage
- Actions in case of breach of agreement

IT Vendors

- IT vendors are prohibited from accessing BASIC's "**Information Assets**" (any resource relating to or containing BASIC's and its clients' data) until a contract containing security controls is fully signed.
- IT vendors and partners must ensure that organizational records are protected, safeguarded, and disposed of securely.

- In cases where the IT Vendor compliance with BASIC's Information Security Program cannot be enforced (for example vendors that operate a subscription-based service provision model, i.e. Microsoft), BASIC must ensure that those vendors have Policies and that the principles indicated in those policies align with that of our own.

IT vendor Contracts

Formal contracts that address relevant security and privacy requirements must be in place for all third parties that process, store, or transmit confidential data or provide critical services. The following must be included in all such contracts:

- Acknowledgement that the third-party is responsible for the security of BASIC's data that it possesses, stores, processes, or transmits.
- Use of key controls to ensure the protection of organizational assets – e.g. physical controls, controls for protection against malicious code, physical protection controls, controls to protect integrity, availability and confidentiality of information, controls to ensure the return or destruction of Information Assets after their use, controls to prevent copying and distributing information.
- Define how intellectual property rights are regulated.
- Responsibilities for responding to direct and indirect security incidents including timing as defined by service-level agreements (SLAs).
- Requirements for the return or destruction of data upon contract termination.
- Geographic limits on where data can be stored or transmitted.

Information Security

Objectives

BASIC expects that information, as defined hereinafter, in all its forms - written, spoken, recorded electronically or printed - will be protected from accidental or intentional misuse, unauthorized modification, destruction or disclosure.

Information Security Requirements

BASIC has identified its information security requirements by utilizing different methods, and will ensure the results of the identification are documented, reviewed and acknowledged by all third-party suppliers/vendors

Methods

- Policies and regulations
- Incident reviews

Factors

- Access provisioning and authorization processes.
- Protection needs of assets, especially in terms of availability, confidentiality, and integrity.
- Other security controls (e.g. interfaces to logging and monitoring).

Protect BASIC's Assets

Intellectual Property

BASIC's intellectual property rights (e.g. trademarks, copyrights, trade secrets, and "know-how") are valuable assets. Unauthorized use can lead to their loss or significant loss of value. You must comply with all intellectual property laws, including laws governing the fair use of copyrights and trademarks. You must never use RigER's trademarks or other protected information or property for any business or commercial venture without written permission from the BASIC.

Data Protection & Retention

BASIC requires that:

- Data is handled and protected according to its classification requirements and following approved encryption standards, if applicable.
- Only services that are required to achieve the business objective or function must be used.
- All privileged access to BASIC information must be logged.

All data of BASIC that is in possession of or operated by a third-party supplier/vendor must be shielded from loss, destruction, falsification, and unauthorized access or release in alignment with legislative, regulatory, contractual, and business obligations.

If a third-party supplier/vendor operates a subscription-based service provision model (i.e. a Cloud Service Provider), BASIC will solicit information regarding the security measures in place for the protection of records collected and stored in the cloud that are pertinent to BASIC's utilization of third-party supplier/vendor's services. Such service providers utilized by BASIC must disclose information about the safeguarding measures for records they gather and store that relate to BASIC's use of their services.

Data in Transit

Necessity

Data must only be transferred where strictly necessary for effective business processes.

Transfer Factors

Before choosing the method of data transfer, the following must be considered:

- Nature, sensitivity, confidentiality, and value of the information
- Size of data being transferred
- Impact of loss during transit

All data transmitted electronically must use the latest versions of applicable cryptographic protocols (i.e. SSL/TLS).

Data Deletion

Stored sensitive data that is no longer required must be properly deleted in accordance with BASIC's business objectives, applicable laws and regulations, and relevant third-party supplier/vendor's contractual obligations. A record of such deletion will be kept.

BASIC will accept the following methods of deletion: overwriting, wiping, physical destruction of media.

Version	**Date**
1.0	January 30, 2026