BIZAGI TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

1. Definitions:

1.1. Capitalized terms used but not defined in this document will have the meaning assigned to them in the Bizagi Cloud- Automation Services Terms and Conditions and the Bizagi Cloud- Studio Collaboration Terms and Conditions and the Bizagi Cloud- Modeler Collaboration Terms and Conditions, as applicable.

2. Security Standards:

2.1. Workforce Security:

2.1.1. Data repositories containing Customers Data shall be maintained by Bizagi Authorized Personnel who have passed sufficient background investigations that revealed no occurrences of criminal convictions or fraud.

2.1.2. Bizagi implements adequate procedures for the clearance, authorization, supervision, training and termination of workforce members.

2.2. Data Security:

2.2.1. Customers Data will be stored in encrypted form. Encryption solutions will be performed at rest and in transit, using available and proven encryption technologies. Those measures prevent reading of data from the physical media by potential attackers, and protect communication between components of the Cloud Services and the database, and communication of end users when accessing the Cloud Services.

2.2.2. Confidentiality, integrity and accessibility of Customers Data will be secured with administrative, technical and physical measures that align with industry-accepted level of security.

2.3. Information Access Management:

2.3.1. Bizagi shall implement policies and procedures for granting access to platform components, establishment, documentation, review, and modification of user's right of access to those components, as well as procedures to verify that a person or entity seeking access to them is the one claimed.

2.3.2. In terms of authentication the Cloud Services support integration with Identity Management services by means of industry renowned standards.

2.3.3. Identity managers in the Cloud Services shall provide secure sign-in capabilities including termination of session after a predetermined time of inactivity and users are encouraged to use a strong password policy and best practices for account settings such as: passwords maximum and minimum age, password minimum length and complexity requirements, password history validation, maximum number of login attempts and account lockout policies, and idle sessions timeout, among others.

2.4. Server Security:

2.4.1. Maintenance of a secure environment for the Customer includes the timely application of patches, fixes and updates to operating systems, services, and applications as employed by the Cloud Services.

2.4.2. Bizagi has established and follows server configuration guidelines and processes with the intent to prevent unauthorized access to Customers Data.

2.4.3. Bizagi has established and follows configuration change management procedures for its servers containing Customers Data.

2.4.4. Bizagi has established and follows backup and restore procedures for servers containing Customers Data as well as retrieval of Customer's data policies and service level agreements.

2.4.5. Data repositories containing Customers Data have isolation measures which endeavor to ensure that:

2.4.5.1. There is no access from one Customer's environment to any other Customer's environment.

2.4.5.2. There is no access from a Customer's environment to anything outside its scope, including its host machine.

2.5. Network Security:

2.5.1. The following applies to all Cloud Services:

2.5.1.1. Network architecture must be designed to limit site access and restrict the availability of information services that are considered to be vulnerable to attack.

2.5.1.2. Application network traffic is limited to standard network ports solely on an as needed basis.

2.5.1.3. Customer's Data transmitted to and from the network shall be sent over encrypted medium or an encrypted format.

2.5.1.4. Application and database servers have proper segregation following industry-accepted practices.

2.5.1.5. Network architecture implements isolation for the different Customer's environments which control that:

2.5.1.6. There is no communication between a Customer's network to eavesdrop traffic on another Customer's network;

2.5.1.7. Traffic cannot be faked to another network.

2.5.2. The following applies only to the Bizagi Cloud Automation Services:

2.5.2.1. Private IP network addresses are used within the network utilized by the service.
The network architecture utilizes multi-layer firewalls with all network access logged and reviewed on a regular basis.

2.5.2.2. Firewalls provide network packet filtering that endeavor to ensure that an untrusted machine cannot:

- **a.** Generate spoofed traffic;
- **b.** Receive traffic not addressed to it;
- **c.** Direct traffic to protected infrastructure endpoints; or
- **d.** Send nor receive inappropriate broadcast traffic.

2.6. Physical Security:

2.6.1. Data centers have an established physical security policy which includes:

2.6.1.1. 24x7 site monitoring; and

2.6.1.2. Site entry control system using multi-factor authentication, in order to gain access to server areas;

2.6.2. Internal site activity monitoring conducted 24x7 using video and environmental sensing technology including:

2.6.2.1. Humidity and moisture control;

2.6.2.2. Fire and smoke detectors;

2.6.2.3. Fire alarms and extinguishing agents; and

2.6.2.4. Logs of all user access to the service's data center.

2.6.3. Activity logging:

2.6.3.1. Where technically and commercially feasible, for systems, data repositories, and network infrastructure devices, Bizagi will maintain logs of its activity.

2.6.3.2. The Cloud Services include monitoring of the Cloud Services availability, resource consumption and performance. Operations staff is alerted to pre-stablished events.

2.6.3.3. With respect to Bizagi Cloud Automation Services, Studio Cloud Services and Modeler Services, Customer has entire control over the Cloud Services authentication and administration. Therefore, procedures to regularly review records of information system activity, such as audit logs, access reports, security incidents, and tracking reports may be implemented by Customer.

3. EXCLUSIONS

3.1. Bizagi shall have no liability for any incidents involving disclosure of Customer Data, which arise out of the inadequate use of Authorized User accounts of Customer's Applications. The Customer is solely responsible for configuring, operating, maintaining, and securing access to Customer Applications and their content, by managing Customer's accounts when using their own identity management system, and enforcing use of strong password policies, enforcing account lockout policies, defining access rights for these accounts, and configuring adequate session expiration.