DATA PROCESSING AGREEMENT

This Data Processing Agreement (“DPA”, “Agreement”) forms part of the master agreement between Customer and Bitrix, Inc. (“Bitrix24”) to reflect the parties’ agreement for the provision of the Processor Services (as amended from time to time) and processing of Customer’s Personal Data in accordance with the requirements of the Data Protection Legislation.
This Data Processing Agreement will be effective from the Effective Date.
If you are accepting this Data Processing Agreement on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to this Data Processing Agreement; (b) you have read and understand this Data Processing Agreement; and (c) you agree, on behalf of Customer, to this Data Processing Agreement. If you do not have the legal authority to bind Customer, please do not accept this Data Processing Agreement.

APPLICATION OF THIS DPA

This DPA will only apply to the extent that the Data Protection Legislation applies to the processing of Customer Personal Data, including if:

(a) the processing is in the context of the activities related to Customers registered through the domain names Bitrix24.eu, Bitrix24.de, Bitrix24.pl, Bitrix24.ua and Bitrix24.fr

(b) The default data processing activities related to Customers registered through the domain names Bitrix24.com, Bitrix24.in, Bitrix24.es, Bitrix24.com.br, Bitrix24.tr, Bitrix24.cn, Bitrix24.kz, Bitrix24.ru and Bitrix24.by are not subject to this DPA. Please contact our helpdesk services for more information for data processing location changes https://helpdesk.bitrix24.com/ticket.php

(c) the processing is in the context of the activities of an establishment of Customer in the EEA; and/or
(d) Offering services to data subjects who are in the EEA
(e) If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Bitrix24 entity that is party to the Agreement is party to this DPA.
This DPA shall not replace any previously applicable agreements relating to their subject matter (including any data processing amendment or data processing addendum relating to the Processor Services)
If there is any conflict or inconsistency between the terms of this DPA and the Terms of Service (https://www.bitrix24.eu/terms/), the DPA will govern. Subject to the amendments in this SPA, the Terms of Service remain in full force and effect.

THE PARTIES HEREBY MUTUALLY AGREE AS FOLLOWS:

1. INTRODUCTION

This DPA reflect the parties' agreement on the terms governing the processing and security of Customer Personal Data in connection with the Data Protection Legislation.

2. DEFINITIONS AND INTERPRETATION

"Affiliates" means any entity which is controlled by, controls or is in common control with Bitrix24.

"Bitrix24" means the Bitrix Inc Group entity that is a party to this DPA and its Affiliates engaged in the Processing of Personal Data.

"Customer Personal Data" means personal data that is processed by Bitrix24 on behalf of Customer as part of Bitrix24 provision of the Processor Services.

"Data Incident" means a breach of Bitrix24 security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data on systems managed by or otherwise controlled by Bitrix24. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"Data Protection Legislation" means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

"Effective Date" means, as applicable:
(a) 25 May 2018, if Customer clicked to accept or the parties otherwise agreed to this DPA before or on such date; or
(b) the date on which Customer clicked to accept or the parties otherwise agreed to this DPA, if such date is after 25 May 2018.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"Notification Email Address" means the email address (if any) designated by Customer, via the user interface of the Processor Services or such other means provided by Bitrix24, to receive certain notifications from Bitrix24 relating to these Data Processing Terms.

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic cultural or social identity;

"Processing of personal data" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ("Process", "Processes" and "Processed" shall have the same meaning).

"Security measures" means measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing as described in the document (or the applicable part dependent on what Services Customer purchases from Bitrix24), as updated from time to time, and accessible via the link in Appendix 2.

"Processor Services" means the provision of maintenance and support services, consultancy or professional services and the provision of software as a service or any other services provided under the Agreement where Bitrix24 Processes Personal Data of Customer.

"Sub-processors" means third parties authorized by Bitrix24 to have logical access to and process Customer Personal Data in order to provide parts of the Processor Services and any related technical support.

"Term" means the period from the Effective Date until the end of Bitrix24 provision of the Processor Services to Customer under the Agreement.
The terms "Data controller", "Data subject", "Personal data", "Processing", "Data processor" and "Supervisory authority" as used in this DPA have the meanings given in the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 Roles and Regulatory Compliance; Authorization.
2.1.1 Processor and Controller Responsibilities. The parties acknowledge and agree that:
(a) Appendix 1 describes the subject matter and details of the processing of Customer Personal Data;
(b) Bitrix24 is a processor of Customer Personal Data under the Data Protection Legislation;
(c) Customer is a controller or processor, as applicable, of Customer Personal Data under the Data Protection Legislation; and
(d) each party will comply with the obligations applicable to it under the Data Protection Legislation with respect to the processing of Customer Personal Data;
(e) Customer shall, in its use or receipt of the Services, Process Personal Data in accordance with the requirements of Data Protection Legislation and Customer will ensure that its instructions for the Processing of Personal Data shall comply with Data Protection Legislation. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.
2.2 Authorization by Third Party Controller. If Customer is a processor, Customer warrants to Bitrix Inc that Customer's instructions and actions with respect to Customer Personal Data, including its appointment of Bitrix Inc as another processor, have been authorized by the relevant controller.
2.3 The parties agree that with regard to the Processing of Personal Data, Bitrix24 or members of the Bitrix24 Group will engage Sub-processors pursuant to the requirements set forth in Section 7 "Sub-processors" below.
2.4 By entering into this Data Processing Agreement, Customer instructs Bitrix Inc to process Customer Personal Data only in accordance with applicable law: (a) to provide the

Processor Services and any related technical support; (b) as further specified via Customer's use of the Processor Services (including in the settings and other functionality of the Processor Services) and any related technical support; (c) as documented in this Data Processing Agreement; and (d) as further documented in any other written instructions given by Customer and acknowledged by Bitrix24 as constituting instructions for purposes of this Data Processing Agreement.
2.5 Deletion on Term Expiry. On expiry of the Term, Customer instructs Bitrix24 to delete all Customer Personal Data (including existing copies) from Bitrix24 systems in accordance with applicable law. Bitrix24 will comply with this instruction as soon as reasonably practicable and within a maximum period of 90 days, unless United States, EU or EU Member State law requires storage.

3. DURATION OF THIS DPA

This DPA will take effect on the Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Customer Personal Data by Bitrix24 as described in this DPA.

4. RIGHTS OF DATA SUBJECTS

4.1 To the extent Customer, in its use or receipt of the Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Legislation, Bitrix24 will (taking into account the nature of the processing of Customer Personal Data and, if applicable, Article 11 of the GDPR) assist Customer in fulfilling any obligation of Customer to respond to requests by data subjects, including (if applicable) Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by providing the functionality of the Processor Services;
4.2 Bitrix24 shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment, restriction, deletion or exercising any other rights under the GDPR of that person's Personal Data. Bitrix24 shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. Bitrix24 shall provide Customer with cooperation and assistance in relation to handling of a Data Subject's request for access to that person's Personal Data or exercising any other rights under the GDPR, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through its use or receipt of the Services.

5. PERSONNEL

5.1 Bitrix Inc shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and are subject to obligations of confidentiality as described in Appendix 2 and such obligations survive the termination of that persons' engagement with Bitrix Inc.
5.2 Bitrix Inc shall ensure that Bitrix24 Group's access to Personal Data is limited to those personnel who require such access to perform the Agreement.

6. DATA SECURITY

6.1 Bitrix24 shall maintain administrative, physical and technical safeguards for protection

of the security, confidentiality and integrity of Personal Data, such measures are described in Appendix 2 to this DPA.
6.2 Bitrix Inc Security Measures. Bitrix Inc will implement and maintain technical, physical and organisational measures to protect confidentiality and integrity of Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access as described in Appendix 2 (the “Security Measures”). As described in Appendix 2, the Security Measures include measures: (a) to help ensure the ongoing confidentiality, integrity, availability and resilience of Bitrix24 systems and services; (b) to help restore timely access to personal data following an incident; and (c) for regular testing of effectiveness. Bitrix24 may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.
6.3 Security Compliance by Bitrix24 Staff. Bitrix24 will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-processors to the extent applicable to their scope of performance, including ensuring that all persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality as described in Appendix 2.
6.4 Bitrix24 Security Assistance. Customer agrees that Bitrix24 will assist Customer in ensuring compliance with any obligations of Customer in respect of security of personal data and personal data breaches, including (if applicable) Customer’s obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:
(a) implementing and maintaining the Security Measures in accordance with the Appendix 2;
(b) complying with the terms of Section 8 (Data Breaches); and
(c) providing Customer with the Security Documentation;

7. SUB-PROCESSORS

7.1 Consent to Sub-processor Engagement. Customer specifically authorizes that Bitrix24 Affiliates may be retained as Sub-processors and Bitrix24 and its Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Service. Bitrix24 and Bitrix24 Affiliates have entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.
7.2 List of Current Sub-processors and Notification of New Sub-processors. Bitrix24 shall make available to Customer the current list of Sub-processors for the Services identified in Appendix 1 of the Standard Contractual Clauses attached hereto. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location, available for Customer on Bitrix24 Website (also accessible via (Bitrix24 Infrastructure and Sub-processors).
7.3 Requirements for Sub-processor Engagement. When engaging any Sub-processor, Bitrix24 will:
(a) ensure via a written contract that:
(i) the Sub-processor only accesses and uses Customer Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this DPA); and
(ii) if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR are imposed on the Sub-processor; and

(b) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Sub-processor.

7.4 Objection Right for New Sub-processors.

When any new Sub-processor is engaged during the Term, Bitrix24 will, at least 10 days before the new Sub-processor processes any Customer Personal Data, inform Customer of the engagement (including the name and location of the relevant sub-processor and the activities it will perform) by sending an email to the Notification Email Address.

Customer may object to any new Sub-processor by notifying Bitrix24 promptly in writing within five (5) business days after receipt of Bitrix24 notice. In the event Customer objects to a new Sub-processor, Bitrix24 will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Bitrix24 is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order with respect only to those Services which cannot be provided by Bitrix24 without the use of the objected-to new Sub-processor by providing written notice to Bitrix24. Bitrix24 will refund Customer any prepaid fees covering the remainder of the term of such Order following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

8. DATA INCIDENTS.

8.1 Incident Notification. If Bitrix24 becomes aware of a Data Incident, Bitrix24 will: (a) notify Customer of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimise harm and secure Customer Personal Data.

8.2 Details of Data Incident. Notifications will describe, to the extent possible, details of the Data Breach, including steps taken to mitigate the potential risks and steps Bitrix24 recommends Customer take to address the Data Incident.

8.3 Delivery of Notification. Bitrix24 will deliver its notification of any Data Incident to the Notification Email Address or, at Bitrix24 discretion (including if Customer has not provided a Notification Email Address), by other direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for providing the Notification Email Address and ensuring that the Notification Email Address is current and valid.

8.4 Third Party Notifications. Customer is solely responsible for complying with breach notification laws applicable to Customer and fulfilling any third party notification obligations related to any Data Incident.

8.5 No Acknowledgement of Fault by Bitrix24. Bitrix24 notification of or response to a Data Incident will not be construed as an acknowledgement by Bitrix24 of any fault or liability with respect to the Data Incident.

9. INSPECTIONS OF COMPLIANCE

9.1 To demonstrate compliance by Bitrix24 with its obligations under this DPA, and upon Customer's request, Bitrix24 will provide more detailed information on the security measures described in the Appendix 2 to the standard contractual clauses: Security Measures for review by Customer.

9.2 Upon Customer's request, and subject to the confidentiality obligations set forth in this DPA, Bitrix24 shall make available to Customer that is not a competitor of Bitrix24 (or Customer's independent, third-party auditor that is not a competitor of Bitrix24) information regarding Bitrix 2 compliance with the obligations set forth in this DPA and the security measures as described in the Appendix 2 to the standard contractual clauses: Security

Measures. Customer may contact Bitrix24 to request an on-site inspection of the architecture, systems and procedures relevant to the protection of Personal Data at locations where Personal Data is stored. Customer shall reimburse Bitrix24 for any time expended by Bitrix24 or its third-party Sub-processors for any such on-site inspection at the Bitrix24 then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Bitrix24 shall mutually agree upon the scope, timing, and duration of the inspection in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Bitrix24, or its third-party Sub-processors. Customer shall promptly notify Bitrix24 with information regarding any non-compliance discovered during the course of an inspection.

10. DATA PROTECTION IMPACT ASSESSMENT

Upon Customer's request, Bitrix24 will assist Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including (if applicable) Customer's obligations pursuant to Articles 35 and 36 of the GDPR, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Bitrix24. Bitrix24 shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks.

11. DATA TRANSFERS

11.1 Data in Bitrix24.eu, Bitrix24.de, Bitrix24.pl, Bitrix24.ua and Bitrix24.fr domain zones is hosted inside the European Union in Frankfurt, Germany with Amazon Web Services data centers, which are fully GDPR compliant - https://aws.amazon.com/blogs/security/...dpr-ready/

11.2 The default data processing activities related to Customers registered through the domain names Bitrix24.com, Bitrix24.in, Bitrix24.es, Bitrix24.com.br, Bitrix24.tr, Bitrix24.cn, Bitrix24.kz, Bitrix24.ru and Bitrix24.by are not subject to this DPA. Please contact our helpdesk services for more information for data processing location changes https://helpdesk.bitrix24.com/ticket.php

11.3 Data Storage and Processing Facilities. Customer agrees that Bitrix24 may store and process Customer Personal Data in the United States of America and any other country in which Bitrix24 or any of its Sub-processors maintain facilities. Bitrix24 will ensure that the level of security in these countries is as described in this DPA.

12. GOVERNING LAW

The Clauses shall be governed by the law of Virginia, United States of America

13. CHANGES TO THIS DPA

13.1 Bitrix24 may change this DPA if the change:

(a) is expressly permitted by this DPA

(b) reflects a change in the name or form of a legal entity;

(c) is required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency; or

(d) does not: (i) result in a degradation of the overall security of the Processor Services; (ii) expand the scope of, or remove any restrictions on, Bitrix24 processing of Customer Personal Data; and (iii) otherwise have a material adverse impact on Customer's rights under this DPA, as reasonably determined by Bitrix24.

13.2 Notification of Changes. If Bitrix24 intends to change this DPA, Bitrix24 will inform Customer at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental

regulator or agency) before the change will take effect by either: (a) sending an email to the Notification Email Address; or (b) alerting Customer via the user interface for the Processor Services. If Customer objects to any such change, Customer may terminate the Agreement by giving written notice to Bitrix24 within 30 days of being informed by Bitrix24 of the change.

CUSTOMER	BITRIX, INC.
Signature:_____	Signature: 
Legal Name:_____	Print Name: Dmitry Valyanov
Print Name: _____	Title: President
Title: _____	Date: 05/24/2018
Date: _____	

APPENDIX 1: SUBJECT MATTER AND DETAILS OF THE DATA PROCESSING

SUBJECT MATTER

Bitrix24 provision of the Processor Services and any related technical support to Customer.

DURATION OF THE PROCESSING

The Term plus the period from expiry of the Term until deletion of all Customer Personal Data by Bitrix24 in accordance with this Data Processing Agreement.

NATURE AND PURPOSE OF THE PROCESSING

Bitrix24 will process including collecting, recording, organizing, structuring, storing, retrieving, using, disclosing, erasing and destroying) Customer Personal Data for the purpose of providing the Services and any related technical support to Customer in accordance with this Data Processing Agreement. The services include the following: Social Intranet, Project Management and Tasks, Chat and Video, Document Management and Bitrix24.Drive, Calendars, Mail, CRM, Sites, Open Channels, Contact center, Telephony, Time management, CRM marketing, Workflows, eCommerce.

TYPES OF PERSONAL DATA

Customer Personal Data may include the types of personal data described below:

- personal details
- location country, city, state and region
- online identifiers
- device identifiers
- personal images
- lifestyle and social circumstances
- details of goods and services
- financial details
- education and employment details
- special category data

CATEGORIES OF DATA SUBJECTS

Customer Personal Data will concern the following categories of data subjects:

- data subjects about whom Bitrix24 collects personal data in its provision of the Processor Services; and/or
- data subjects about whom personal data is transferred to Bitrix24 in connection with the Processor Services by, at the direction of, or on behalf of Customer.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES: SECURITY MEASURES

As from the Terms Effective Date, Bitrix24 will implement and maintain the Security Measures set out in this Appendix 2. Bitrix24 may update or modify such Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.

1. DATA CENTERS & NETWORK SECURITY

(a) DATA CENTERS.

INFRASTRUCTURE

Bitrix24 uses Amazon Web Services to store and analyze data, including AWS Cloud infrastructure in Europe (Frankfurt) Region and Europe (Ireland) Region.

PHYSICAL SECURITY

Employee Data Center access. Physical data center access is provided only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

Third-party data center access. Access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.

MONITORING & LOGGING

Data Center access review. Access to data centers is regularly reviewed. Access is automatically revoked when an employee's record is terminated in Amazon's HR system. In addition, when an employee or contractor's access expires in accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon.

Data Center Access logs. Physical access to AWS data centers is logged, monitored, and retained. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis.

Data Center Access monitoring. Data centers are monitored by global Security Operations Centers, which are responsible for monitoring, triaging, and executing security

programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.

SURVEILLANCE & DETECTION

CCTV. Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

Data Center entry points. Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

Intrusion detection. Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication. Alarms are immediately dispatched to 24/7 AWS Security Operations Centers for immediate logging, analysis, and response.

REDUNDANCY

Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AVAILABILITY

AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

BUSINESS CONTINUITY PLAN

The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

PANDEMIC RESPONSE

AWS incorporates pandemic response policies and procedures into its disaster recovery planning to prepare to respond rapidly to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources, and activation of a crisis management plan to support critical business operations. Pandemic plans reference international health agencies and regulations, including points of contact for international agencies.

ASSET MANAGEMENT

AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

MEDIA DESTRUCTION

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

OPERATIONAL SUPPORT SYSTEMS

Power. AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

Climate and temperature. AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

FIRE DETECTION AND SUPPRESSION

Fire detection and suppression. AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

LEAKAGE DETECTION

In order to detect the presence of water leaks, AWS equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

INFRASTRUCTURE MAINTENANCE

Equipment maintenance. AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

Environment management. AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.

GOVERNANCE & RISK

Data Center risk management. The AWS Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

Third-party security attestation. Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.

(b) **Networks & Transmission**.

Data Transmission. Bitrix24 Datacenters are connected via private links protected by AWS Network firewalls to provide secure data transfer. This is designed to protect the confidentiality, integrity and availability of the network and prevent data from being read, copied, altered or removed without authorization during electronic transfer.

Intrusion Detection. Intrusion detection is intended to prevent ongoing attack activities and provide adequate information to respond to incidents. Bitrix24 intrusion detection involves:

(a) Employing intelligent detection controls at data entry points; and

(b) Employing technologies that automatically remedy certain dangerous situations.

Data Breach Response. Bitrix24 monitors a variety of communication channels for security breaches, and Bitrix24 security personnel will react promptly to known incidents.

External Attack Surface. Bitrix24 considers potential attack vectors and incorporates appropriate purpose built proprietary technologies into external facing systems.

Encryption Technologies. Bitrix24 uses HTTPS encryption (also referred to as SSL or TLS connection).

2. PERSONNEL SECURITY

Bitrix24 personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Bitrix24 conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Bitrix24 confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Personal Data are required to complete additional requirements appropriate to their role. Bitrix24 personnel will not process Customer Personal Data without authorization.

3. SUBPROCESSOR SECURITY

Before onboarding Subprocessors, Bitrix24 conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Bitrix24 has assessed the risks presented by the Subprocessor then, subject always to the requirements set out in Section 7 the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.