Technical And Organizational Security Measures

The following information describes the technical and organizational security measures implemented by Journyx (also "we," "us," or "our" in the description below).

1. Encryption

Our Services use industry-accepted encryption methods for data in transit and data at rest, using 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum. Journyx employs SSL everywhere for customer data. No HTTP access is allowed, only HTTPS. The current SSL key is a sha256 RSA implementation at a length of 4096 bits. Replicated data (failover, backups) are encrypted in transit and at rest.

2. Ensuring Ongoing Confidentiality, Integrity, Availability and Resilience

Only tested, generally available (GA) product releases are deployed to production. Should any customer wish to perform their own system staging or testing, they may do so either on a dedicated test system purchased separately, or on a Journyx-owned test system (usually during a Journyx professional services engagement), rather than on the production customer environment.

Journyx cloud operations are single tenant. Each client site has its own database, and all customer data is contained within that database. No other Journyx installation can connect to, or communicate with, the database.

Journyx IT routinely updates internal and production environments to meet evolving security standards. Vulnerable software is identified and patched, or removed depending upon the situation.

Backups are performed nightly for Journyx production, failover and office networks. For our customers' cloud system production data located in the United States, offsite backups are securely stored at Journyx headquarters on a backup server where they are then transferred to secure offsite media. For such data located in the EEA, offsite backups are securely stored on a non-public S3 container in the Frankfurt region. Journyx maintains roughly 90 days of customer cloud backups. Cloud system data may be returned to a customer after termination of the service upon request; thereafter, it is securely deleted in accordance with our data deletion and destruction policies and procedures.

Journyx implements controls to maintain the confidentiality of Customer Services Data in accordance with the Agreement. All Journyx employees and contract personnel are bound by the terms of their employment or contractor agreement and our policies to comply with confidentiality obligations.

3. Restoring Confidentiality, Integrity, Availability and Resilience in the Event of an Incident

We operate failover data centers, geographically separated from the production data centers, to handle technical or natural events that might disrupt production operations. The Journyx failover data center in the United States operates on an Amazon Web Services (AWS) center located more than 500 miles from the production center, and resides on a different electrical grid; the failover data center in the EEA is located more than 300 miles from the EEA production center. The failover center also operates on Amazon Web Services.

We monitor for and respond to data Security Incidents that may impact availability or access in accordance with our data Security Incident response plan. In the event an exigent threat is discovered to the systems on which the Services run, Journyx moves immediately to correct such problems, issuing customers an Emergency Maintenance Notification as soon as possible after a resolution has been identified. We take similar measures to restore availability and access to our internal (office) networks, to protect business operations continuity.

Journyx has business continuity and disaster recovery plans in place, and tests them at least annually. The Journyx Services recovery plans have a recovery time objective (RTO) of within 24 hours after Journyx's declaration of a disaster, and a recovery point objective (RPO) of 24 hours.

4. Testing, Assessing and Evaluating the Effectiveness of Measures and Controls

Journyx performs quarterly security assessments internally, including vulnerability assessment and penetration testing. Additionally, third parties are engaged annually to provide an external assessment. Results of security assessments are not made available to external parties, for reasons of security. The results are examined by our external auditors, and they inform our information asset risk assessment, which is also provided to our audit firm annually.

We run security scans on our application during pre-release testing. Industry-accepted tools and standards such as OpenVAS, Metasploit and OWASP among others are used to assess and guide security of the application during development.

Journyx has an internal audit process that examines our internal controls for data protection quarterly. Any deviations, deficiencies or areas for improvement are documented and the issues timely resolved. The results of these audits are provided to our external auditors during our annual external audit.

5. User Identification and Authorization

Journyx ensures, via segregation of duties and systems, that Journyx-internal testing systems and customer production systems are fully separated. Only authorized IT staff have access to production systems, data, or environments.

Upon initial setup of a customer's Journyx solution, a single administrator-level user account is created for each customer system, and that username/password combination is released to the customer, along with instructions to change the password. Some customers engage Journyx Professional Services to assist in configuration and population of customer data; however, access to the customer site and data is controlled solely by the customer.

Except for authorized IT staff performing ongoing production environment operations, no Journyx staff can access customer data in a Journyx production system unless their job role permits them to provide services to the customer. In such cases, access is granted only at the customers express, properly-documented request, and only if the services or assistance requires access to customer data. Upon completion of the services/assistance, staff are required to relinquish their account to the customer's control.

User access rights and security groups are reviewed during quarterly internal audits, and annually by external auditors. Requests to grant access rights must be formally documented and approved. Only HR may request access rights for new staff. In the event of a job role change, the individual's manager must document and request from IT any access rights modifications. HR notifies IT of staff terminations; IT executes an access rights checklist for all terminations.

We require that staff whose job role includes obtaining and/or granting access to Customer Services Data (such as customer support or professional services) validate any request from Customer staff or any third party for access to Customer Services Data. Customers are required to provide Journyx with the contact information for Customer's authorized system administrator, who is the point of contact with Journyx regarding access rights to and within the Journyx Services and to Customers Data. The customer, and not Journyx, administers user accounts in the Journyx Services.

Journyx allows no logical access to the Journyx production or failover centers with the following exceptions:

- SSL/TLS access to the Journyx web application interface
- FTP/SCP/SFTP access to the secure Journyx FTP server for file transfers
- SSH access to the infrastructure itself from Journyx headquarters only
- Encrypted replication access to the infrastructure from Journyx headquarters
- Encrypted replication access between Journyx production and Journyx failover centers
- Access to the Journyx infrastructure using AWS tools including but not limited to the AWS Console and AWS API methods
- Encrypted access within and between Journyx production and failover centers

SSH access is controlled via secure RSA keys in addition to username and password, and such access is restricted to the Journyx IT department.

Web and API access to a customer's installation of the Journyx cloud software is controlled solely by the customer. Journyx internal controls prohibit our employees from accessing any customer's data without explicit authorization from the customer. Upon customer authorization, only Journyx employees in our support, professional services or IT teams may have access to customer data, and only to the extent necessary to respond to the customer's requests and instructions. This is further enforced by Journyx IT procedures that lock the support administrator account used by Journyx Support for each customer installation daily. That account can only be unlocked by the customer (within the product itself) by use of a customer administration account, or by Journyx IT (at the express request of the customer) for customer support purposes.

6. Protection of Data During Transmission and Storage

Services use industry-accepted encryption methods for data in transit and data at rest, using 128-bit TLS Certificates. Journyx employs SSL everywhere for customer data. No HTTP access is allowed, only HTTPS. The current SSL key is a sha256 RSA implementation at a length of 4096 bits.

Services use industry-accepted encryption methods for data at rest, using 2048-bit RSA public keys at a minimum.

7. Physical Security of Data Centers and Offices

At our office locations, Journyx employs 2 separate RFID access points (main building as well as Journyx leased space). Doors remain secured and may only be accessed via RFID 24x7. Journyx also employs a monitored alarm system which notifies the police when triggered.

AWS data centers are strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication (2FA) a minimum of two (2) times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions. Each data center has redundant electrical power systems that are available twenty-four (24) hours a day, seven (7) days a week. Uninterruptible power supplies and on-site generators are available to provide back-up power in the event of an electrical failure.

8. Event Logging

Journyx uses redundant industry-standard network monitoring and notification software packages, configured to alert Journyx IT of situations from moderate to critical on a 24x7 basis and escalate critical notifications if they have not been addressed in a specified timeframe. It monitors Journyx internal networks, production environments, and failover environments in real time to ensure that Journyx-provided services are functioning optimally.

9. System Configuration Control

The systems Journyx uses to provide the Services can be configured only by authorized IT staff. The configuration specification is documented in the IT operating procedures manual. Formal change management procedures are followed.

Journyx has 3 types of maintenance events: Emergency, Required and Optional. An email will be sent to the contact of record a minimum 2 business days prior to required and optional patches, hotfixes and upgrades. In the event of an emergency maintenance, the contact on record will be notified as soon as feasible.

10. Internal IT and IT Security Governance and Management

Journyx has a dedicated IT team to manage our information assets and systems. The team follows documented operating procedures that are reviewed and approved by executive management as needed, but no less often than annually. Journyx also has a dedicated data security team that includes IT staff; the team follows a documented data Security Incident response plan (DSIRP) that is reviewed and approved by executive management as needed, but no less often than annually. The DSIRP defines how IT must monitor for, document, and remediate any vulnerabilities, policy violations, suspicious activity, compromised systems, or unauthorized access.

Journyx has a dedicated risk management program, including risks to information assets and systems. Risk management and IT staff are part of the audit team, who conduct the internal audit program and who also facilitate and support the annual external audit. IT reports on data protection monthly to the executive team.

Journyx maintains a data security and information use policy; all staff are required to read, understand, and sign agreement to follow the policy. The policy is provided at the time of hire, and must be reviewed annually thereafter. All staff are required to attend security training annually.

Journyx maintains a privacy office. A privacy program is in place with documented operational procedures. The privacy office recommends and implements policy and procedures, and handles privacy inquiries including data subject inquiries.

11. Certification and/or Assurance of Processes and Products

The Journyx Services use AWS as the data center infrastructure provider. AWS audits to the relevant standards including ISO and SOC2, among others. Journyx office (business) operations audit to the appropriate SOC 1 SSAE Type II standard. Our ongoing internal audit function assures the quality of our processes and controls.

We have a team dedicated to quality assurance of the Services. We follow a rigorous software development lifecycle process, reviewed annually by external auditors and designed to assure quality throughout the development lifecycle.

12. Data Minimization

Within 30 days of subscription or contract termination, customers may request return of their Customer Data submitted to the Journyx Services (to the extent data have not been deleted previously by the customer). Journyx will make the data securely available to the customer for download.

Starting on the 31st day after subscription or contract termination, or as may be otherwise specified in our Agreement with a customer, Customer Data submitted to the Journyx Services is subject to secure deletion or overwriting. Our standard data deletion procedures will remove the data at some time between the 31st and the 90th day after termination. Physical media used to store Customer Data within the Journyx Services during the subscription or contract term are not removed from the data centers unless the media are being deprovisioned. Deprovisioned media are securely wiped before removal, except where legal requirements demand otherwise.

13. Data Quality

Data input validation may be implemented by the Customer where appropriate in the Services to prevent manual input errors. Data handling features of the Services are rigorously tested prior to release. Role based data access rights ensure data may not be modified except by authorized users, and as permitted by Customer's system configuration. Data integrity routines are implemented at the database level to assure data integrity.

Journyx performs data security, privacy, and compliance risk assessments of our sub-processors and any third party vendors that handle personal information and/or system data. We enter into agreements with its customers and service providers that are appropriate to the data and information the other

party will process; the agreement terms contain obligations to ensure confidentiality and data protection, as well as the lawfulness, fairness and transparency of processing.

14. Limited Data Retention

Within 30 days of subscription or contract termination, customers may request return of their data submitted to the Journyx Services (to the extent data have not been deleted previously by the customer). Journyx will make the data securely available to the customer for download.

Starting on the 31st day after subscription or contract termination, or as may be otherwise specified in our Agreement with a customer, data submitted to the Journyx Services is subject to deletion. Our standard data deletion procedures will remove the data at some time between the 31st and the 90th day after termination. Physical media used to store data within the Journyx Services during the subscription or contract term are not removed from the data centers unless the media are being deprovisioned. Deprovisioned media are securely wiped before removal, except where legal requirements demand otherwise.

Journyx maintains policies and procedures to strictly limit retention of personal information and customer services data, where the data are not required by law to be retained.

15. Accountability

Journyx implements appropriate technical and organisational measures for data protection. We assure and can demonstrate the proper design and operation of the measures by means of our external audit of our system of controls. Our infrastructure provider, AWS, similarly undergoes external audits of controls, and can produce audit reports that attest to design and operation of controls.

Journyx maintains documentation on what personal data we process, and the purpose, duration, and means of processing, which is described in our Agreement and our privacy policies. Documented processes and procedures for data protection are reviewed and updated as needed, but at least annually, and approved at the executive level. We have a dedicated data privacy team; the leader is integrated our planning and operations, and reports to the CEO.

16. Data Portability and Erasure

Customers have the ability to use self-service features to export data from the Services, in accordance with the permissions set in place by the Customer. Customers may request a return of their entire Customer Services Data set from Journyx within 30 days of termination of the Agreement; Journyx will provide it in a standard format mutually agreeable to the parties.

Customers may choose, in accordance with their internal policies and legal obligations, to delete their Customer Services Data using the features of the Services. Except as otherwise specified in our Agreement with the Customer, beginning 31 days, but no later than 90 days after termination of the Agreement with Journyx, Journyx will delete Customer Services Data remaining in the Services.

17. Sub-Processor Assistance to the Processor and Controller

Journyx enters into agreements with sub-processors that contain substantially similar obligations to those in this DPA. The sub-processors of Customer Services Data are obliged to confidentiality, to

implement data protection measures, notify Journyx in the event of a data Security Incident, assist us as needed to discharge our obligation to assist a data controller in responding to data subject requests or incident reports, and to process data only as per our instructions, which instructions will be in accordance with the terms of this DPA. AWS is a subprocessor that cannot access or process Customer Services Data, but AWS meets all sub-processor obligations that apply with respect to the infrastructure services they provide.

18. Processor Assistance to the Controller

Journyx will assist the controller in accordance with Applicable Data Protection Law and the terms of this DPA and the Agreement. Journyx has a dedicated privacy team and a documented privacy program with procedures in place to assist the controller, in particular with data subject inquiries. Because Customer, and not Journyx, administers the Journyx Services, Journyx will determine the controller of the data that are the subject of the inquiry, promptly direct any such data subject inquiries we receive to the controller, and assist controller in responding in accordance with applicable law.