Workflow Science
the cloud work company

UNCLASSIFIED

G-Cloud 9

Service Definition

Workflow Science Limited

Process Automation Suite

1st April 2017

Contents

1 Overview 4

2 Definitions 4

3 Service Description 4

3.1 Overview 4

3.2 Modeller 5

3.3 Automation Service 5

3.4 Portal 5

4 On-boarding and Off-boarding 5

4.1 On-boarding 5

4.2 Off-boarding 5

5 Disaster Recovery 6

5.1 Data back-up and restore 6

5.2 Platform restoration 6

6 Service Management 6

6.1 Our responsibilities 6

6.2 Your responsibilities 6

7 Service Levels 6

8 Service Credits 7

9 Training 7

10 Information Assurance 7

10.1 Data in transit protection 7

10.2 Asset protection and resilience 7

10.3 Separation between consumers 7

10.4 Governance framework 7

10.5 Operational security 8

10.6 Personnel security 8

10.7 Secure development 8

10.8 Supply chain security 8

10.9 Secure consumer management 9

10.10 Identity and authentication 9

10.11 External interface protection 10

10.12 Secure service administration 10

10.13 Audit information provision to consumers 10

10.14 Secure use of the service by the consumer 11

11 Technical Requirements 11

11.1 Modeller 11

11.2 Portal 11

12 Trial Service 11

13 Ordering and Invoicing 12

14 Term and Termination 12

15 Terms and Conditions 12

1 Overview

A process is the ordered collection of related tasks that produces a product, service or desired outcome. Processes can be simple with just a few steps or they can be complex with many steps, complicated ordering and numerous dependencies.

Processes are found in every type and size of business; they define how products are made and sold, or how services are delivered; they also support day-to-day activities, such as chasing customer debt or booking annual leave. Whether the tasks within the processes are carried out by humans (such as employees or customers) or by systems, automating and managing these processes will deliver significant business benefits.

2 Definitions

The following definitions are used in this document:

Personal Data: personal data as defined in the Data Protection Legislation;

Service: the Automation Service provided by Workflow Science Limited, as described in this document;

Service Charge: the monthly subscription level based charge payable by you in return for receipt of the Service;

Service Provider(s): a third party organisation, business or individual offering service to others;

Subscription Charge: the monthly comprising of a Service Charge and Usage Charges;

Usage Charges: those charges incurred as a result of the execution of any task within an activated process in the Automation Service;

User(s): your employees whom you authorise to access the Service, and all third parties, including partners, suppliers and customers to whom you make the Service available;

We, **us** or **our**: means Workflow Science Limited;

You or **your**: you, the customer, or one of your Users; and

Your Data: all information of whatever form (whether or not Personal Data) relating to you and/or any third party provided by Users arising out of or in connection with their access to and/or use of the Service and all information of whatever form (whether or not Personal Data) provided by Service Providers.

3 Service Description

3.1 Overview

Our **Process Automation Suite** is a secure and scalable enterprise-grade cloud-based solution designed to firmly place you in control of rapidly creating and automating your processes.

We have reduced or eliminated the traditional technical barriers, meaning that non-technical people who best understand the processes within a business are able to easily and

cost-effectively create, change or evolve processes to meet the needs of customers, modify or launch new products or services, and rapidly respond to changes in environmental or regulatory conditions.

Together our **Process Automation Suite** comprises a process modelling application ("Modeller"), a process automation service ("Automation Service") and a web-based work and management portal ("Portal"), as further outlined below.

3.2 Modeller

The Modeller is our unique process modelling application that you download and install on a Windows or Mac computer. It allows you to create processes, create resources and define information flows in an intuitive easy-to-use, drag-and-drop graphical environment without requiring any IT or technical expertise.

The Modeller supports full team working, access rights and version management.

3.3 Automation Service

Our Automation Service stores, manages and controls execution of your processes; schedules and makes work available to all resources that are involved in a process, including humans, systems and information stores; and provides centralised process and resource model storage and versioning for the Modeller. You access the Automation Service through the Portal to control the operation of your processes, get access to your human work and view dashboards providing business intelligence, reports, up-to-the-minute statistics, audit and billing information.

3.4 Portal

Our Portal is a web application accessed via a standard web browser. It connects to the Automation Service, enabling you to view and manage your processes, create and administer users, and access reports, analytics and business intelligence. The Portal is where users access the tasks allocated to them by your running processes, creating a work-list for each user. Just like our Modeller application, the Portal can be used by anyone regardless of their level of IT skills.

4 On-boarding and Off-boarding

4.1 On-boarding

We have a fully automated customer on-boarding process accessible on our public website (https://www.workflow-science.com). Once you have entered all the information we need to capture, the on-boarding process takes around 60 seconds to complete, after which you will be able to log in to your account and start creating your first process.

4.2 Off-boarding

We have a fully automated customer off-boarding process accessible to all customers by logging into the Portal (https://www.workflow-science.com/portal/app). The off-boarding process takes around 60 seconds to complete. You are responsible for exporting your data and any other information prior to starting the off-boarding process.

5 Disaster Recovery

5.1 Data back-up and restore

We carry out automated back-ups of all your data and configuration once per day. These automated back-ups are used solely to protect against loss of your data in the event of a significant failure in one or more components of our system. These back-ups do not provide you with the ability to selectively restore older versions of your data as mitigations where either you or one of your processes accidentally overwrites certain data.

If you use one or more of our information stores to store your data, you can back-up (and restore) any such data yourself through the use of the Customer Interface (see §10.11.1).

5.2 Platform restoration

In the event of a significant failure in one or more components of our system, we will take all reasonable steps to restore the Service to a fully operational state, using data from the most recent automated data back-up.

6 Service Management

6.1 Our responsibilities

We will manage our Automation Service and use all reasonable steps to ensure the Service is fully operational in accordance with §7 (Service Levels).

6.2 Your responsibilities

You are responsible for managing those failures associated with your use of services provided by Service Providers accessed through the Service Provider Interface (§10.11.2) by your running processes.

There are a number of different types of failures that can occur when using Service Providers, including:

[1] failures due to a lapse in subscription or depleted credit;
[2] authentication and/or authorisation failures due to changes in passwords, keys or other security credentials; and
[3] other changes that materially affect the behaviour of the interface to the Service Providers' service.

All failures will be reported in the Portal; you will be notified in accordance with those notification rules you configure in the Portal.

7 Service Levels

We take all reasonable measures to ensure our Service operates at a minimum availability of 99.9%, excluding:

[1] scheduled maintenance, where necessary and as notified to you giving a minimum of twenty four (24) hours' notice; and
[2] events outside our reasonable control, including but not limited to Force Majeure.

8 Service Credits

Service credits are your sole and exclusive remedy and our sole and exclusive liability for failure to meet Service Levels. Service credits are a pro rata credit against the Service Charge for that period of time the Service is not available to you during any given month.

9 Training

We can provide training on use of our **Process Automation Suite**. A quotation for training can be provided on request.

10 Information Assurance

We follow the guidance of CESG "Cloud Security Guidance: Summary of Cloud Security Principles" updated 08 December 2015 and have in place the following security procedures and technical and operational measures to safeguard your data.

10.1 Data in transit protection

We use industry standard Secure Sockets Layer (SSL) technology that encrypts and secures all information (including passwords and payment information) that you exchange with our Automation Service through use of the Modeller, the Portal or by any other means through the Customer Interface (see §10.11.1).

You are responsible for all information exchanged by your processes with Service Providers over the Service Provider Interface (see §10.11.2) and you should ensure that the correct technical security measures are configured to protect the confidentiality of your data passed over this interface.

10.2 Asset protection and resilience

Our Automation Service is hosted in the EU by our third party supplier Amazon AWS. We refer you to http://aws.amazon.com/security/ for further information on this principle.

10.3 Separation between consumers

Our Automation Service is a multi-tenancy platform supporting multiple customers and has been designed to ensure the isolation of customer information at all levels, such that:

[1] all customer security credentials, rights assignments and security policies are isolated and stored within a dedicated security realm;
[2] all customer information internally in transit (within the Automation Service) is uniquely tagged with a Customer identifier;
[3] all customer information at rest is isolated and stored within logically separate databases; and
[4] each and every service and information request is subject to identity authentication and authorisation checks (see §10.10, Identity and authentication).

10.4 Governance framework

We receive security and vulnerability alerts and we monitor security and vulnerability bulletins, including US-CERT National Cyber Awareness System. We use such information to continually

assess the threats to our Service and implement any necessary mitigations, either through scheduled maintenance or immediate updates, dependent upon impact and severity.

10.5 Operational security

10.5.1 Configuration and change management

We operate a configuration management system for all assets, including software and configuration.

All software is built and labelled so that it is uniquely identifiable. Deployment of built software is controlled through the Administration Interface (see §10.11.3) using automated deployment agents.

Deployment of all configuration, including security related configuration such as firewall rules and security policies, is controlled through the Administration Interface (§10.11.3) using automated deployment agents.

All changes, such as customer feature requests, defects and mitigations, are recorded, assessed and scheduled through planning according to priority and/or urgency and impact.

10.5.2 Vulnerability management

We manage vulnerabilities through a combination of inputs from §10.4 (Governance framework) and §10.5.4 (Incident management). Assessment and scheduling of mitigations is in accordance with §10.5.1 (Configuration and change management).

10.5.3 Protective monitoring

We operate a real-time monitoring and management system that tracks activity on all external interfaces, including all authentication and/or authorisation failures. Our personnel are automatically notified of all abnormal activity and/or patterns.

10.5.4 Incident management

We operate an incident management process to log, assign and diagnose incidents based upon urgency and impact, and to restore Service operation quickly with minimum disruption.

10.6 Personnel security

All employees undergo basic screening as part of pre-employment checks.

10.7 Secure development

All our software development is carried out in-house following development guidelines. Each change to software and/or configuration is assessed in terms of its impacts on access management policies, access rights and/or firewall rules.

Our software engineering team have a dedicated development environment on which assessments of functional and non-functional (including security) correctness and fit for purpose are tested, and we have a robust release management process in place.

10.8 Supply chain security

We use a single third party, Amazon AWS (with services hosted in the EU). For further information relating to Amazon AWS' security conformance and credentials, we refer you to http://aws.amazon.com/security/.

10.9 Secure consumer management

10.9.1 Authentication of consumers to management interfaces and within support channels

Management requests are only accessible via the Customer Interface, accessed through our Portal. Access to all management requests is subject to authentication and authorisation, as per §10.10 (Identity and authentication).

10.9.2 Separation and access control within management interfaces

As per §10.10 (Identity and authentication), you may enhance the security on any or all management requests through the use of Multi-Factor Authentication. For example, you could mandate that all management requests MUST originate from a given location or IP address.

10.10 Identity and authentication

User access to our Automation Service through the Customer Interface is managed by an off-the-shelf identity management, authentication, authorisation and entitlement system. Further support is provided for federated identity.

10.10.1 Authentication

All users accessing the Service are required to authenticate using:

[1] as a minimum, a company identifier, username and password; and, optionally (configurable),
[2] additional factors including knowledge factors, possession factors, inherence factors, time factors and location factors.

Authentication can be configured to lock out a user after a (configurable) number of unsuccessful authentication requests. Locked out users will need to have their account unlocked by your (nominated) administrator.

10.10.2 Sessions

Once a user is authenticated, a session is established for exclusive use by that user, subject to:

[1] a user can have at most one (1) active session (configurable);
[2] a session is established for a maximum of two (2) hours (configurable) after which the session will be terminated and the user will need to re-authenticate; and
[3] if a session is inactive for a period of thirty (30) minutes (configurable) the session will be terminated and the user will need to re-authenticate.

10.10.3 Authorisation

Authorisation is managed through Role-Based Access Control (RBAC). Using the Portal, you create roles and assign one or more rights (to access a given resource) to each role. Users (also created in the Portal) are assigned to one or more roles, effectively assigning (indirectly) rights to each user. These rights are enforced on each and every request for service or information.

10.10.4 Standards

Authentication and authorisation standards supported by our Automation Service include OAuth, SAML, OATH, SecurID, OpenID and HOTP.

10.11 External interface protection

Our Automation Service supports the following external interfaces:

10.11.1 Customer Interface

The Customer Interface is used by you to access the Automation Service. Confidentiality of information exchanged on the Customer Interface is protected as set out in §10.1 (Data in transit protection) and each such request is subject to those authentication and authorisation mechanisms set out in §10.10 (Identity and authentication).

10.11.2 Service Provider Interface

The Service Provider Interface is a collection of interfaces that enables your processes to request service from and exchange information with Service Providers.

Our firewalls and security rules block ALL incoming requests on this interface.

Outgoing requests for service from Service Providers and the resulting exchange of information is controlled by you as part of your configuration of the Automation Service.

10.11.3 Administration Interface

The Administration Interface is for use by our personnel only. It is a single point of access for administration of the Automation Service and is controlled via a Bastion Host dedicated solely to service management.

Access to this interface is protected in a number of ways, including:

- restricting access requests by IP address;
- authentication using RSA 2048 bit SSH key-based log-in;
- authentication re-enforcement by username and password; and
- all information exchanged across the interface is encrypted using industry standard Secure Sockets Layer (SSL) technology.

Further security certificates and credentials are required once connected to the Bastion host to access any server, infrastructure or data.

10.12 Secure service administration

Access to servers, infrastructure and your data by us is controlled through a Bastion Host dedicated solely to service management (see § 10.11.3, Administration Interface). Provision of the necessary credentials and access rights to our personnel is strictly based on need and uses fine grained control of rights, restricting access only to those component parts (of the server, infrastructure or your data) required by our personnel to carry out their duties from time to time.

10.13 Audit information provision to consumers

All authentication requests, both successful and unsuccessful, are audited and logged. All requests to access services and information are audited and logged together with details of the service and information that was accessed or denied access to.

Audit logs are accessible by you via the Portal. Each log entry contains, as a minimum:

- the date and time of each request;
- the service or information requested;

- whether the request was permitted or denied;
- the user identifier making the request;
- the result or outcome of the request; and
- the IP address (or location) from where the request was received.

10.14 Secure use of the service by the consumer

Whilst we take all reasonable steps to protect and safeguard your data (as set out more generally in this document), you are and remain responsible for the protection of your data. Whilst we do not provide detailed security guidance, we highlight below some of the key features of our Service that may help you in fulfilling your responsibilities:

[1] review and configure the maximum number of simultaneous sessions a user can have with the Service as appropriate (see §10.10.2);
[2] add additional factors into user authentication and authorisation, including restricting time and location from which users can log in to the Service (see §10.10);
[3] assign users only to those roles required for them to carry out their duties (see §10.10);
[4] review and configure password aging as appropriate (see §10.10);
[5] review and configure maximum session timeouts and idle timeouts as appropriate (see §10.10.2); and
[6] ensure appropriate configuration of the Service Provider Interface to protect the confidentiality of your data that is exchanged by your processes with Service Providers.

11 Technical Requirements

11.1 Modeller

Our Modeller application is compatible with the following Operating Systems:

[1] Windows XP;
[2] Windows Vista (32-bit and 64-bit);
[3] Windows 7 (32-bit and 64-bit);
[4] Windows 8 (32-bit and 64-bit); and
[5] Mac OSX 10.8+

11.2 Portal

Our Portal is compatible with the following web browsers:

[1] Internet Explorer 10+;
[2] Firefox 4+;
[3] Chrome 38+
[4] Safari 6+;
[5] Opera 11+;
[6] Edge 20+;
[7] Android native browser 4.2+;and
[8] iOS native browser 6.0+.

12 Trial Service

We offer a sixty (60) day fully functional, no obligation trial of our Service free of charge[1]. Full conditions are available in our Terms and Conditions (WFS G-Cloud 9 Terms and Conditions.pdf).

13 Ordering and Invoicing

Your Service subscription will commence on receipt of our order confirmation after you initiate the customer on-boarding process (see §4.1, On-boarding).

The Subscription Charge for our Service will be invoiced on a monthly basis on the calendar day corresponding to the commencement of your Service (the "Billing Period").

You will pay the invoiced amount in full within thirty (30) days of the date of each invoice.

You may cancel your subscription to the Service in accordance with §14 (Term and Termination).

14 Term and Termination

Provision of our Service is for an initial period of one (1) month and thereafter continues automatically from month to month.

You may terminate your subscription to the Service by initiating the customer off-boarding process (see §4.2, Off-boarding) at any time. You will continue to have access to the Service through to the end of your monthly Billing Period after which your access to the Service will be removed.

We may terminate your subscription to the Service without liability on the provision of one (1) month's written notice.

15 Terms and Conditions

Provision of our Service is strictly subject to our Terms and Conditions (WFS G-Cloud 9 Terms and Conditions.pdf), which shall prevail in the event of any conflict with this document.

[1] No payment details are required to sign up for a free trial.