Taskize Connect Policies - Definitions

Change Date: 9 October 2019

Review Date: April 2023

Definitions relating to the provision of Services to Clients

“Agreement” means the Order Form including, by reference, the Terms and Conditions and the Policies.

“Client” means the entity named as the Client in the Order Form.

“Client Data” means the Personal Data, data, information and/or material inputted by the Client or any user to the Services or otherwise provided by it or any user in connection with the Service or provided to Taskize.

“Order Form” means the order form entered into by the Client (as amended or replaced);

“Policy” means the policies of Taskize (including any updates or replacements) available on www.taskize.com.

“Service” means all the services provided by Taskize to the Client where the Client is the Data Controller, including the software as a service application called Taskize Connect (and Service shall be construed accordingly).

“Sanctions” refer to sanctions laws, regulations, embargoes and restrictive measures enacted or enforced by the European Union, the United Nations Security Council, where applicable the United States Office of Foreign Assets Control (OFAC), the United Kingdom, and all other applicable jurisdictions.

Definitions relating EU Data Protection Legislation

“DP Laws” means all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679) (“GDPR”); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended; any other European Union legislation relating to personal data and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).

The terms, "Commission", "Controller", "Data Subject", "Personal Data", "Processing", "Processor" shall have the same meaning as in DP Laws.

“Data Controller” means “Controller”.

“Data Processor” means ”Processor”.

All other defined terms have the same meanings as those given in the Terms and Conditions.

## End of Document ##

Taskize IT Security Policy

Change Date: April 2021

Review Date: April 2023

Introduction

This Policy uses terms from Taskize Policy Definitions and additionally defines terms used only in this Policy.

Services Covered

This Policy describes the architecture of, the security, and the administrative, technical and physical controls applicable to the Services provided by Taskize.

Taskize Infrastructure

Taskize deploys and operates its software at a third-party data centre and services are provided by Amazon Web Services (AWS).

Physical access and physical security to data centres is managed by AWS. Access for anyone other than to AWS employees and contractors is prohibited.

The infrastructure that AWS provides Taskize is designed and managed in alignment with security best practices and recognised IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- SO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

Their ISO27001 certificate is available at:
https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf

AWS also manages the destruction of decommissioned equipment: "*When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent Client data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All* *decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.*"

Taskize Client Data is presently located in AWS data centres in the European Economic Area. Clients of Taskize may choose other or additional geographic region(s) to locate their data, subject to our agreement and the availability of AWS facilities in the region, which will incur additional charges.

Client Data is not moved between regions without a Client's consent.

If a Client communicates with only its own staff, the Client Data remains only in the region(s) selected by the Client.

When a Taskize client uses the Service to interact with other Taskize client(s), the data of those interactions may be copied to the regions elected by the other Taskize clients being communicated with (e.g. a US bank may elect to have its data located in the USA, EEA and Singapore) so that those messages may be received by those clients.

System Security

All internal communication channels within Taskize are encrypted.

Taskize uses firewalls control inbound and outbound traffic for every server instance in the environment. By default, all inbound traffic is denied, explicit rules must be added to allow inbound traffic.

Public corporate IP address ranges may be added to an allowlist as one of a several options available to enforce multi-factor authentication to the Taskize Production Service. External traffic is not permitted to connect to application components prior to successful login.

A File Integrity Monitoring (FIM) solution is deployed on all Production servers to provide Host-Based Intrusion Detection. FIM logs are aggregated by a Security Information and Event Management (SIEM) tool, which is actively monitored by Taskize Security. Taskize servers run operating systems hardened to CIS standards at server deployment as part of the Taskize automated system deployment processes.

Scalable load-balancers provide mitigation of Distributed Denial of Service (DDoS) attacks by rapidly scaling load-balancer and security layers to absorb and deflect the additional load of an attack.

Administrative access to Production Services is controlled by both network design and access controls.

All access to production servers must go through bastion servers, access to these is via layered virtual private networks and secure shells with least privilege. Only employees authorized in the Taskize Identity Management System can establish connections to the bastion servers, and further access to servers is controlled and provisioned based on role requirements. Access levels are regularly reviewed. All connections to bastion servers is logged, access logs are regularly reviewed by Taskize staff.

The Taskize platform is monitored for security events by a SIEM tool which looks for indicators of compromise. In the event that a security incident (which may be less than a breach) occurs, the Security Incident Response procedure will be followed to limit the impact of the incident. Logs are digitally signed and access to the log storage is limited and recorded.

In the event of a confirmed security breach the Head of Cyber Security will work with Taskize senior management to make all reasonable efforts to communicate with impacted Clients within 48 hours of detection.

Each Client should provide Taskize with contacts to be informed in the event of a security breach. Each affected Client will be provided with updates on the progress of any investigation or remedial action by senior management at Taskize.

Application Security

Only entities which have received authorisation from Taskize may access Taskize. .

SAML2 is optionally supported for clients to remove the need for Taskize to hold user credentials and to automate Client staff registration and single sign-on using the Client's own corporate directory.

Taskize only allows HTTPS for Production Service communications. The access network is the Internet.

The servers are found at *.taskize.com which should be permitted by Client firewalls and proxies to enable Production, integration, test and recovery server access.

Note that the Taskize global network scaling and resilience implementation means that its server farm does not resolve to a pool of static IP addresses and that proxy-server DNS name-filtering must be used instead.

The Taskize Security team actively monitors vulnerability reporting feeds. Regular vulnerability scans are performed against the Production systems. Decisions to patch or not are made by assessing the threat and impact of each vulnerability.

A weekly Production maintenance window is reserved for the deployment of upgrades, patches, and system maintenance.

All deployments of upgrades and patches are tested in lower environments prior to deployment in Production.

Automated tests are performed in the lower environments to ensure that the upgrades and patches do not negatively impact the system. Once deployed in Production, smoke tests are performed to ensure the system performs as expected, as well as checks that any vulnerabilities which were meant to be addressed by the patches have been resolved when possible.

Reliability and Backup

System components, load balancers, web servers and application servers are configured in a redundant configuration. There is no single point of failure and recovery and failover is automatic, except for database and certain middleware components where failover is manually directed by operations staff following defined procedures.

All Client Data submitted to the Taskize system is stored on a primary database server with a remote passive node for increased availability.

All Production databases are backed-up on a nightly basis.

In addition to automated backups, manual full backups of critical Production databases are taken prior to upgrades, maintenance, or significant changes to the databases to allow for rapid recovery or rollback.

Disaster Recovery

Taskize has disaster recovery plans in place and tests them at least once per year.

The Taskize Services utilize secondary facilities that are separate and independent from the primary data centres, along with required hardware, software, and Internet connectivity, in the event Taskize Production facilities at the primary data centres were to be rendered unavailable.

The Service disaster recovery plans currently have the following target recovery objectives:

- restoration of the Service within 4 hours after Taskize's declaration of a disaster
- maximum Client Data loss of 15 minutes
- excluding, however, a disaster or multiple disasters causing the compromise of two or more data centres at the same time, in which case the recovery time will be 48 hours

This disaster recovery plan applied to Production Services only, and exclude integration, test, evaluation and development environments.

## End of Document ##

Taskize Record Retention Policy

Change Date: April 2021

Review Date: April 2023

In its business operations Taskize collects and stores records of many types and in a variety of different formats. This policy applies to all systems, people and processes that constitute Taskize information systems.

Principles

Principles regarding record retention and protection:

- Records are held in compliance with English Law and the contractual requirements which apply to Taskize and the Client
- Records are not held for any longer than required
- The protection of records in terms of their confidentiality, integrity and availability are in accordance with their security classification
- Records remain retrievable in line with business requirements

Record Retention Policy

The following descriptions relate to the Production Services only.

Client Data

Client Data is stored by Taskize for as long as the Client maintains its Subscription to Taskize, unless otherwise stated below.

Bubbles

Bubbles are records of interactions within or between clients of Taskize.

Taskize technology ensures that each Client participating in the Bubble has a separate record of the Bubble. For example, if there are four participants from one Client participating in a Bubble, there is one logical copy of the Bubble. If there are four participants from four Clients participating in a Bubble, there are four discrete logical copies of the Bubble. Think of this as a separate journal being maintained on behalf of each Client.

By default, each Bubble is retained in the on-line Service on behalf of its participating Clients for a period of 13 months, unless stated otherwise in the Agreement.

Backups

The Production Service is backed up at least daily.

The backups include all Client Data.

Backups are retained for at least a period of 90 days.

Backups are encrypted.

User records

A small amount of personal identifying data is used by the Service (e.g. name, work email address, work telephone number, job title).

This data is retained in the online system for the longest of:

1) The duration that the user is an Authorized User of the Service, where that information has been made known in advance of becoming an Active User.
2) The duration that the user is an Active User of the Service.
3) The duration that the Service has an online record of any Bubble that the user participated (up to 13 months, or as otherwise agreed with the Client).
4) A period of 90 days past the deletion of the above Bubbles in the backup.

If a user leaves and re-joins the Service within 13 months they may be associated with the account from when they left.

If they leave and re-join after 13 months, they may be associated with a new account.

If a user moves from one Client to another Client (a change of employer), their record at the new Client will be entirely separate to any previous Client.

Anonymized user records

Taskize collects meta-data about how the system is used in order to improve the Service, provide related Services and to provide anonymised reporting to enable Clients to better understand their use of the Service.

After a user record has been removed from the system, activity data may be retained for up to five years for aggregate reporting but only once all information identifying the user has been removed from these records.

Bubble meta-data

Taskize collects meta-data about how the Service is used in order to improve the Service, provide related Services and to provide anonymised reporting to enable Clients to better understand their use of the Service.

To enable this, high-level meta-data including anonymised participants, causes, durations and resolutions may be retained for up to five years after the content of a Bubble has been deleted.

Non-Production environments

For the avoidance of doubt, non-Production environments include any capability containing the descriptions “Test”, “Development”, “Integration”, “Pilot”, “Evaluation” or similar.

Non-Production environments are not backed up unless agreed otherwise. Data from non-Production environments is not retained for longer than 30 days after the cessation of the respective environment.

Record Destruction

Once records have been kept for the defined period, they are securely destroyed in a manner that ensures that they can no longer be accessed or used.

## End of Document ##

Client Record Retention Policy

Change Date: 9 October 2019

Review Date: April 2023

Taskize Services includes communications and task management but is not a long-term data archival service (unless otherwise specifically agreed with the Client).

Taskize therefore requires that each Client downloads and stores any information that they may require to satisfy the requirements of the regulatory authorities applicable to it.

Principles

The key principles of the Client Record Retention Policy are:

- Taskize Clients are, or are responsible for in relation to this Policy, entities which may fall under the jurisdiction of regulators in one or more countries
- Clients are responsible for ensuring they adhere to the data management and retention requirements of their regulator(s)
- Taskize provides facilities which enable Clients to extract archivable records of their activities on Taskize
- Taskize is not a regulated entity

Policy Statements

Client is responsible for:

- downloading any required information extracts from Taskize in a timely manner
- storing the extract in a manner acceptable to their regulator(s)
- retaining the extracts for the duration required by their regulator(s)
- retrieving and displaying the extracts as they require
- responding to, administering and processing requests by their regulator(s).

Client acknowledges that downloaded data may contain:

- information supplied by third parties which have entered into a similar agreement with Taskize
- Personal Data identifying the participants and entities in the downloaded conversations
- information which may be Confidential to it and /or to the third parties.

Client must:

- treat Confidential and Personal Data with the same care that it treats its own confidential information.
- not subject downloaded data to systematic processing and /or analysis of any kind.

- limit its activity with respect to downloaded data only to that required to satisfy the reasonable requests of regulators, auditors and law enforcement agencies.

Taskize disclaims to the maximum extent possible all warranties with regards to the downloaded data.

Data extraction

Data extraction from Taskize by a Client is performed at the Bubble level.

All Bubbles which a Client is actively participating in, or has participated in and which are still stored in Taskize online Service are available for download in the user interface, or programmatically via the API.

Bubbles are extracted as simple files encoded as RFC 5322 / EML format (see http://www.digitalpreservation.gov/formats/fdd/fdd000388.shtml). Attachments to the Bubble which are eligible for export are encoded as attachments to the email.

An alternative structured XML archive format is available for download via the API.

In practice, this means that these files may be simply stored by the Client in a suitable secured computer file system or proprietary email retention system (not supplied) and opened using tools such as Microsoft Outlook (not suppled) or Mozilla Thunderbird (not supplied).

## End of Document ##

Taskize Acceptable Use Policy

Change Date: 9 October 2019

Review Date: April 2023

Introduction

This Policy uses terms from Taskize Policy Definitions.

The Taskize Acceptable Use Policy applies to any user who uses the Service.

Acceptable Use

The Client and its users may only use the Services for the purposes described in its applicable agreement with Taskize.

If Taskize discovers or suspects that a user is using the Service in a way that is prohibited or for business purposes incompatible with the Acceptable Use, Taskize may, at its sole discretion, do one or more of following:

a. disable or remove the user concerned;
b. remove, suppress, and/or redact all or part of the content of the Bubble(s) affected;
c. remove, suppress, redact and/or disable access to the Bubble(s) affected; or
d. in extreme and persistent cases, terminate the Service to the Client and charge Client any applicable fees for the Service used.

Prohibited Use

Users shall not use the Service:

- for any illegal, fraudulent, improper or abusive purpose, or in any way that interferes with Taskize's ability to provide high quality services to other clients, prevents or restricts other clients from using the Service, or damages any of Taskize's or other clients' property;
- to send, display, store, process or transmit material that:
  - infringes third party intellectual property rights or violates the rights (such as privacy or publicity) of others;
  - is hate, drug, hacking or phishing related, illegal (or encourages illegal acts), obscene, violent, discriminatory or otherwise objectionable; or
  - includes malicious code (such as virus's, worms, timebombs etc) or unlawful software;
- to imitate or impersonate any other person or entity or create accounts unconnected to an authorised Client user;
- to data mine or harvest any Taskize or related web property to find email addresses or other use account information, or to send unsolicited communications to significant numbers of individuals and/or entities (including Taskize) with whom you have no pre-existing relationship with;

- to access any Taskize product or service, or other service or website, in a manner that violates the terms for use of or access to such service or website, or that violates any applicable industry standards, third party policies or requirements that Taskize may communicate to its users;
- to conduct or forward multi-level marketing, such as pyramid schemes and the like;
- to perform significant load or security testing (and/or publish the results) without first obtaining Taskize's written consent;
- to remove any copyright, trademark or other proprietary related notices contained in or on the Service or reformat or frame any portion of the web pages that are part of the Service's administration display;
- to attempt, cause, permit, or authorise the copying, modification, creation of derivative works, translation, reverse engineering, decompiling, disassembling, or hacking of the Service or any software and/or hardware used in conjunction with the Service, or part thereof, or otherwise attempt to defeat, disable or circumvent any protection mechanism related to the Service;
- to access the Services for the purposes of web scraping, web crawling, web monitoring, or other similar activity through a web client that does not take commercially reasonable efforts to identify itself via a unique user agent string describing the purpose of the web client and obey the robots exclusion standard (also known as the robots.txt standard), including the crawl-delay directive;
- in any manner that would disparage Taskize; or
- if themselves or their associated Client entity is under Sanctions that are applicable to Taskize given the nature of its business and activity.

Client shall not wilfully and persistently breach the system usage levels set out in their Agreement.

## End of Document ##

Taskize Data Privacy Policy

Change Date: April 2021

Review Date: April 2023

Introduction

> *Taskize's public website at https://www.taskize.com is covered by the separate Taskize Web Privacy Policy which is unrelated to the Service.*

This Policy uses terms from Taskize Policy Definitions.

An important note for people who use Taskize

Client staff and contractors must be made aware that their use of Taskize has personal data implications for them which may extend beyond the United Kingdom and European Economic Area.

Taskize may use the name, work phone number, work email address and job title of users to attribute their actions within Bubbles.

A copy of the content of a Bubble is shared with each of the entities (third parties) which participated in it and may be held outside Taskize and outside the European Economic Area. However, the third parties have each agreed with Taskize to hold any such data securely for audit and regulatory purposes only not to subject the data to automated processing or analysis.

For comparison, similar data sharing happens in many email communications between companies. Taskize offers stronger protections than email to protect this data.

If you do not accept the above, you must not use Taskize.

Compliance with DP Laws

For Services, Taskize is the Data Processor and Client is the Data Controller.

Taskize complies at all times with the applicable DP Laws. For more information regarding our minimum obligations and rights to the Client relating to our role as Data Processor, please refer to our Terms and Conditions.

Additional Information regarding Data Processing

Processing of Personal Data

Taskize will only process Personal Data to the extent required to provide the Services in accordance with the Agreement or in accordance with the Client's explicit instructions.

The subject matter and duration of Processing is set out in the Agreement with the Client.

Types of Personal Data processed by the Services

- Name
- Work Title or Occupation
- Work Telephone Number
- Work Email Address
- Employer
- Other Personal Data that the Client or a user inserts when using the Services.

Categories of Data Subjects

- Any person using, or mentioned during the use of, the Services.

Details of current Sub-Processors

Taskize currently uses the sub-processors specified at www.taskize.com/sub-processors, who are subject to equivalent obligations that are imposed on Taskize under the Agreement with the Client.

Data Subject Rights

Clients have primary responsibility for interacting with Data Subjects, and the role of Taskize is generally limited to assisting Clients as needed.

Access, correction, amendment or deletion Requests

With regards to the Service, Data Subjects should direct all requests for access to, correction, amendment or deletion of its Personal Data to the Client. Taskize shall co-operate with Client to assist such request.

Data Subject Complaints

Data Subjects should lodge all complaints about processing of their respective Personal Data with the relevant Client. Client shall be responsible for responding to all Data Subject complaints except where such Client has disappeared factually, has ceased to exist in law or has become insolvent.

Where Taskize is aware of such a case, it undertakes to respond directly to Data Subjects' complaints within thirty (30) days.

Regulatory & Compliance Complaints

Taskize legal department shall be responsible for handling complaints related to compliance with the Agreement, this Policy and the DP Laws.

Taskize shall, to the extent legally permitted, promptly notify a Client if Taskize receives an inquiry or complaint from a data protection authority in which that Client is specifically named. Upon a Client's written request, Taskize shall provide the Client with cooperation and assistance in a reasonable period of time and to the extent reasonably possible in relation to any regulatory inquiry or complaint involving Taskize processing of Personal Data.

Audits

Taskize and the Client's respective audit obligations are set out in the Agreement with Client.

The following third-party audits and certifications are applicable to the Services.

- ISAE 3402 Service Organization Control 2 Type II (SOC 2 Type II) Internal Verification

Taskize has appointed its Head of Cyber Security (or his successors) to be responsible for overseeing and ensuring compliance with Taskize's data protection responsibilities.

Security Breach Notification

For a description of security breach prevention, detection and notification please see the System Security section of the Taskize IT Security Policy.

Data Protection Officer

Taskize has registered with the UK Information Commissioners Office (ICO), registration reference **ZA182954**.

For data protection enquiries, please contact legal@taskize.com.

## End of Document ##

TASKIZE
MAKE WORK FLOW

Taskize Support Services Policy

Change Date: April 2021

Review Date: April 2023

This Taskize Support Services Policy applies to the service and the support provided by Taskize as part of the Service acquired under the Agreement.

Service Availability

Taskize will make reasonable commercial efforts to make the Taskize Connect Service available 24 x 7. Where scheduled maintenance is required, it may occur on Sundays between 5pm and midnightUK Time.

Taskize Support Services

Taskize is committed to providing best in class support services to its customers.

Taskize Support Services consists of:

- General maintenance releases, selected functionality releases, and documentation updates.
- Program updates, fixes, security alerts, and critical patch updates; and
- Dedicated client support, as detailed below.

Support Level	**Description**
Self-Service (Taskize Help Centre)	• First port of call • Provides fast answers to common questions • Provides proven solutions to common problems • Continuously improved
First Line (Taskize Client Support)	• Receives communications from users regarding problems using the Service • Logs problems in the incident management system • Attempts to resolve the problem • Escalates the problem to an incident where necessary
Second Line (Taskize Technical Operations Support)	• Receives escalated incidents from First Line Support • Updates incident records in the query management system with actions taken • Attempts to resolve the incident • Escalates to the Third Line Support Analyst where necessary
Third Line (Taskize Application Support)	• Receives escalated incident from Second Line Support • Investigates issues, develops fixes and work-arounds

Clients are encouraged to use the Self-Service Support first, since it is available to all Clients free of charge and provides high-quality answers which may be faster than contacting Support.

Client Process to Access Support

Clients are required to establish and maintain processes as necessary to ensure that users have sufficient training and local support in the use of the Service within your organization as it applies to your business.

If after reasonable efforts a Client is unable to diagnose or resolve a problem, a Client or a user may contact Taskize for support via the channels supported by your subscription, which may include one or more of the following:

- Self-Service Help Centre at https://help.taskize.com (must be accessed via Client premises)
- Taskize Support Bubble: Entity - Taskize, Function - IT Support
- Taskize Support Telephone: 0044 (0)20 3874 7224
- Taskize Support Email: support@taskize.com

It is in everyone's interest to ensure smooth running of operations, and Taskize may review service requests logged by users and recommend specific training and/or process changes to help prevent recurring support issues.

Response times

Taskize is committed to responding to all support requests relating to Severities 1 – 3 (which can be logged with Taskize at any time via phone, email or a Taskize Bubble), and all other inquiries that are received through channels supported by your subscription.

Please note however that unless your Agreement provides for enhanced Support Hours, these channels will only be monitored during UK Business hours, excluding weekends and UK holidays.

SaaS Support Target Response Times:

Severity	**Description**	**Target Response**
1 (Critical)	Production issue affecting all users; system unavailability	1 hour
2 (High)	Persistent issue affecting many users; major functionality is impacted; significant performance degradation	2 hours
3 (Medium)	System performance issue or bug affecting some but not all users; or issues for which work arounds are available	4 hours

Severity	Description	Target Response
4 (Inquiries)	Inquiries about routine technical issues; information requests on application capabilities; navigation, installation, or configuration	8 hours

- Response times for Severities 1 - 3 do not vary if you file your Support Request via phone, email or Taskize bubble.
- Taskize does not guarantee resolution times, and a resolution may consist of a fix, workaround, service availability or other solution Taskize deems reasonable.
- Taskize will provide continuous efforts (24x7x365) to resolve Severity 1 and 2 service availability issues until a workaround or resolution can be provided or until the incident can be downgraded to a lower severity.
- While an incident is at Severity 1 or 2, Client should make their representative available to determine if a satisfactory resolution can be quickly achieved.
- Unless your Agreement provides for enhanced support hours, target response times for all levels of Severities are subject to UK business hours only and excludes weekends and UK holidays.

Taskize also continually monitors the Service to ensure disruptions are minimized and any incidents are promptly addressed.

Upgrade/Downgrade of Severity Level

If, during the Support Request process, the issue either warrants assignment of a higher severity level than currently assigned or no longer warrants the severity level currently assigned based on its current impact on the production operation of the SaaS offering, then the severity level will be upgraded or downgraded accordingly to the severity level that most appropriately reflects its current impact.

Escalation

You may escalate an incident which has previously been reported to the Taskize Support team and where progress is not visible or satisfactory. The escalation path is:

1. First level Client Support Management
2. Top level Executive Management

The escalation will be managed by the active Client Support. The first level Client Support Management will review the progress on the incident and feed back to the client on the action taken.

## End of Document ##

Taskize Complaints Policy

Change Date: April 2021

Review Date: April 2023

Taskize make every effort to ensure that our Clients are happy with the level of service and the Services they receive from us.

However, we understand that things can go wrong. We take Client complaints very seriously, and we aim to resolve them quickly and efficiently.

Complaints Process

If you have a complaint about any part of the Service, please contact our Client Service Team by one of the following methods:

Telephone:	+44 20 3874 7224
Email:	complaints@taskize.com
Mail:	Customer Success Taskize Limited 33 Cannon Street London EC4M 5SB

During any discussions, we will protect the privacy of the information disclosed. To ensure the protection of your privacy, we may ask questions to confirm that we are speaking to the right person.

We will acknowledge receipt of your complaint within 2 business days.

We will try to resolve your complaint and keep you informed of any progress of developments.

## End of Document ##

TASKIZE
MAKE WORK FLOW

Taskize Service Update Policy

Change Date: April 2021

Review Date: April 2023

Introduction

This Policy sets out the Service update schedule (for bug fixes and feature releases).

Taskize acknowledges that change requests can come from multiple sources and will require prioritisation and scheduling by it.

The Policy distinguishes between bug fixes, improvements, and feature releases, which will follow separate release cycles.

In both cases, the scheduled maintenance window will be used to deliver the updates (as detailed in the Taskize Support Services Policy).

Release Cycle

Bug Fixing and Improvements

- Issues rated as Critical will be resolved and deployed into production as soon as is commercially reasonable (All other sandbox environments will be "patched" sometime shortly after)
- Issues rated as High will be resolved and deployed into production on twice monthly basis within scheduled maintenance windows
- Issues rated as Medium and below will be prioritised relative to and released with the overall product release schedule.

Feature Releases

- Taskize will log and prioritise feature requests from all clients. An updated record of delivered changes will be made available to all clients.
- Highest priority features will be released into Production on a **quarterly** basis
- By prior arrangement and where your subscription includes access to a Sandbox, feature releases will be made available in client Sandboxes up to **2 weeks** in advance of the Production deployment.

Feature Release Notifications

Taskize aims to make available the list of expected changes for the upcoming Feature Release approximately 3 months ahead of the release. Notification is done via our email and/or via Newsletters, so please ensure we have appropriate email addresses on file.

Taskize follows an Agile Methodology in its product development, but is also conscious of its clients' requirements for stability and a controlled rate of change. Therefore, while the list will identify the maximum features which may be part of the release but Taskize may have to withdraw planned features they are not appropriately ready for release.

## End of Document ##

TASKIZE

MAKE WORK FLOW