Kōrero

Korero / Talent Toolbox

Business Continuity, Security & Data Policies

Contents

Introduction

ICT continuity management supports the overall business continuity management (BCM) process for clients of Korero's software-as-a-service products (or SAAS, referred to hereafter as "services").

BCM seeks to ensure that Korero's services are protected from disruption and that Korero is able to respond positively and effectively when disruption occurs. Continuity management ensures that the services are resilient and can be recovered to predetermined levels within timescales required by and agreed between Korero and its clients.

Due to the nature of Talent Toolbox's purpose and features, it is deemed a non-essential function for businesses using it, so the policies in place offer sufficient protection for clients of Korero, but without going to the levels required by a mission critical service.

Business Continuity Management

In the event of a severe unplanned service disruption, whereby Talent Toolbox is expected to be unavailable for a significant period of time (over an hour), responsibilities and procedures are defined to ensure the right people are involved to enable Korero to respond positively and effectively, and to restore the service to a stable state as quickly as possible.

Disaster Recovery

Procedures and Responsibilities

Technical Director

- When notified about a service disruption, perform an initial diagnosis of the disruption to check for a swift and simple resolution
- Notify all Executive Directors about the disruption so they can keep all clients up-to-date
- Coordinate diagnosis of the root cause of the disruption with the Technical Team, providing an estimated time to the Support Team for when normal service will resume
- Liaise with the hosting provider if the root cause concerns hosting
- Provide guidance to the Technical Team where necessary to ensure a resolution is found as quickly as possible
- Notify the Support Team if normal service will not be resumed within the original estimated time frame
- Understand the root cause and give permission for the proposed solution to be implemented
- Coordinate the testing procedure, to ensure service only resumes once stable and secure
- Notify the Support Team as soon as the system is back online
- After the service is back online, oversee and document:
    - Root cause analysis
    - The effect on the service – total estimated downtime, and any lasting impact on the Talent Toolbox service (including data)
    - Steps taken to bring the service back online
    - Immediate mitigations required
    - Planned mitigations
- Perform a review of the response, examining its effectiveness and identify any areas that could be improved

Technical Team

- Assist the Technical Director in root cause analysis
- Assist the Technical Director in mitigating the issue and resolving any data issues

- Implement any fixes required to restore normal service
- Test the restored service to ensure stability and security before releasing to clients
- Compare data in the database to a backup of the database taken just before the incident begun, to ensure no data has been lost

Support Team

- Brief clients on communications received from the Technical Director regarding the disruption as soon as possible, relaying information on estimates for when normal service will resume, and once the disruption is over and analysis is complete, provide information on what happened, why, and what steps are being taken to prevent the same problem happening again.

Support Team and Testers

- Test the restored service to ensure stability and security before releasing to clients

All of Korero

Notify the Technical Director as soon as a service disruption is noticed or reported by client(s).

Example Scenario: Complete Loss of Primary Datacentre Facility

Talent Toolbox data is very well protected, but in the unlikely event of a complete failure of the primary datacentre, the following procedure is in place to bring the system back online as efficiently as possible.

Formation of the Response Team

The Technical Director forms a Response Team consisting of all available developers, an Support Team member, a Support Team member and a Software Tester (if available).

The Response Team is briefed by the Technical Director on the nature of the problem, facilitates a discussion about likely causes, and assigns responsibilities to team members.

Initial Client Notification

The Support Team notify their clients of the disruption and assure the clients that this is being looked into as a matter of urgency, and that they will be kept up-to-date.

Technical Response

Diagnosis

The Technical Team members will check the status report of the hosting provider, and find that there is a complete failure at the primary data centre. An estimate for when normal service can resume will be provided by the Technical Director to the Support Team, who can then relay that information to their client(s).

Database Testing

The database will automatically failover and an exact replica available immediately at the secondary datacentre. Connectivity should be tested by a developer. Once connected, a data comparison should be performed with the latest backup to ensure the replica is in the state expected.

Web Application Restore

The web applications will be deployed from the latest stable version of the source code, to a new production environment in the secondary datacentre. Any connection changes for databases, file storage locations can be made in the configuration files.

Testing

The web applications will be tested, using a pre-defined procedure to ensure the complete range of features are tested. This step involves both developers and the Software Tester (where available). Once testing is completed successfully, the Technical Director is notified and gives permission to release.

Release

The talenttoolbox.com domain name is pointed to the address of the new production servers, and clients notified by the Support Team that the system is back online.

Review

The Response Team gather together, led by the Technical Director, to discuss how the disaster recovery procedure went, and suggest any improvements to the plan.

An investigation into the cause of the datacentre failure is undertaken by the Technical Director, and the suitability of the hosting provider assessed.

A plan is put in place to restore Talent Toolbox to the primary data centre as soon as is sensible, so that the secondary failovers are available again.

Testing Procedure

The Disaster Recovery plan is practiced regularly to ensure that, in the event of a serious disruption, Korero are able to quickly and efficiently restore Talent Toolbox to the state it was before the disruption.

Korero take advantage of their cloud-based hosting to test disaster recovery in an environment which matches the production environment, i.e. using the same specification of servers, in the same datacentres with the same network etc.

The table below outlines the frequency of testing individual parts of the Disaster Recovery plan. To summarise, the approach taken is to frequently test each component in isolation (e.g. database restore), and to test the entire plan a sensible amount of times per year, or as soon as a change is made to the plan.

Component	Test Frequency
Restoration of nightly database backup from primary file store	Daily
Restoration of nightly database backup from secondary file store	Weekly
Deployment of source code to clean web application servers	Weekly
Point In Time database restoration	Fortnightly
Restoring files to primary data store from secondary data store	Monthly
Complete Disaster Recovery Plan testing	Quarterly

Backup Policies

A comprehensive set of steps are taken to reduce all risks to loss of source code and application data.

Source Code

The source code for Talent Toolbox is managed by a distributed revision control and source code management system. This service is provided by a third party (GitHub). All source code repositories are stored on a minimum of three different servers and an off-site backup.

It's worth noting that no client data is stored in the source code repositories other than some image assets such as logos. Confidential data must not exist in the repositories, and there are multiple levels of protection to ensure this doesn't happen, including pull request based code reviews.

Web Application Hosting Environments

Application Servers

Deployments to production environments are fully automated using a continuous integration server connected directly to the source code management system. All data entered or uploaded by users is saved to a database or to a file store, as opposed to the application servers.

The architecture of Talent Toolbox has been designed for scalability. By combining this with a cloud-based infrastructure for its hosting, it is very easy to create a new instance of Talent Toolbox running on a new web server.

As such, backups of the application servers are not required.

File Storage

The file storage is geo-redundant, replicated to a secondary data centre in a different region to the primary data centre. In the event of a failure in the primary data centre, access to the file storage will automatically failover to the secondary data centre.

Files stored in the file storage will all be uploaded by users of Talent Toolbox. For example, profile pictures, image gallery pictures and cv's. Due to the nature of Talent Toolbox, it should not be used to store files that are critical to the daily functioning of its clients. Because of this, Korero do not routinely test restoring these files from the secondary data centre.

Databases

The best performing service tier is used for the Talent Toolbox database, which also offers exceptional levels of business continuity. This offers:

- Automated Export – scheduled creation of database backups, stored in redundant file storage
- Point In Time Restore - functionality which allows for restoration of the database to a state at any point from the last 35 days
- Geo-Restore - in the event of a datacentre failure affecting the availability of the primary database, Geo-Restore allows us to recover the database using the last available daily backup
- Database Copy – allows for creation of a copy of a database either on the same or different servers in the same or different regions. The copy is transactionally consistent with the source when the database copy operation is complete.
- Geo Replication - a single offline secondary database exists in a different predetermined region than the primary database. The secondary database becomes available to client connections only when the datacentre hosting the primary database fails.

The database hosting platform used mitigates outages due to failures of individual server components, such as hard drives, network interface adapters, or even entire servers. Data durability and fault tolerance is enhanced by maintaining multiple copies of all data in different physical nodes located across fully independent physical sub-systems such as server racks and network routers. At any one time, three database replicas are running—one primary replica and two or more secondary replicas. Data is written to the primary and one secondary replica using a quorum based commit scheme before the transaction is considered committed. If the hardware fails on the primary replica, the database detects the failure and fails over to the secondary replica. In case of a physical loss of a replica, a new replica is automatically created. Therefore, there are always at minimum two physical transactionally consistent copies of Talent Toolbox data in the datacentre.

Database backups are stored in a separate file store with read access to the replicated file store to enable Korero to test restoring of database backups.

Security Plan

Privacy Issues

Talent Toolbox holds data about its clients and their employees. This includes a small amount of personal data, such as names, date of birth and contact details. As a Data Processor our clients do not expect the information they have stored in our system to be shared with anyone else, purposely or accidentally. Every effort is made to ensure clients and their employees' details and feedback are kept secure. Reputational damage could amount from one client seeing another client's information for example, so Talent Toolbox is regularly penetration tested to ensure that this isn't possible. In addition, any PC/laptops used by Korero employees to access personal data are set to automatically install critical security patches, and hard drives are fully encrypted to offer extra protection.

Data Protection

Korero will process personal data in line with the Data Protection Act 2018 (the UK's implementation of GDPR). Personal data will only be used for the purpose it is collected and nothing further. Personal data must not be taken out of the system or out of the office without prior consent. Only staff working within the Technical and Support Teams are permitted to access personal data that is stored. Should further access be required, permission must be sought and granted by the client.

Data Breaches

Introduction

Care should be taken to protect this type of data, to ensure that it is not changed (either accidentally or deliberately), lost, stolen or falls into the wrong hands, and that its authenticity and integrity is maintained.

In the event of a breach, it is vital that appropriate action is taken to minimise associated risks.

What is a breach?

A data breach is an incident in which any of these types of data specified above is compromised, disclosed, copied, transmitted, accessed, stolen or used by unauthorised individuals, whether accidentally or on purpose. Some examples:

- Accidental loss, or theft of equipment on which data is stored
- Unauthorised access to data
- Human error such as emailing data by mistake
- Failure of equipment and hence data held on it

- Hacking attack
- Where information is obtained by deceiving an employee of Korero

Reporting of the breach

Data security breaches should be reported immediately to the Support Team, as the primary point of contact. The report should include full and accurate details of the incident, including who is reporting the incident, what type of data is involved, if the data relates to people, how many people are involved. The Support Team will keep a log of this information, and can be contacted at ask@talenttoolbox.com or 020 7836 6999

Investigation and Risk Assessment

The Technical Director will initialise a Response Team, who will be responsible for investigating data breaches. An investigation will be started within 24 hours of the breach being discovered.

The investigation will establish the nature of the breach, the type of data involved, whether the data is personal data, and if so who are the subjects and how many are involved. Also, it will consider the extent of the sensitivity of the data, and a risk assessment performed as to what might be the consequences of its loss, for instance whether harm could come to individuals or to clients.

Containment and Recovery

The Response Team will determine the appropriate course of action and the required resources needed to limit the impact of the breach. This might require temporarily shutting the system down.

Appropriate steps will be taken to recover data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords. Insert info here

Advice from experts may be sought e.g. a Data Protection specialist.

Notification

The CEO/MD will be notified by the Response Team following a critical data breach involving large amounts of data, or a significant number of people whose personal data has been breached. They will also make an informed decision as to whether affected clients should be notified by the breach. Records of any meetings held about the breach, along with any key decisions, will be kept by Korero.

If a personal data breach has occurred, the Information Commissioner's Office will be notified if necessary, based on the extent of the breach.

Review

Once the breach is contained a thorough review of the event will be undertaken by the Response Team, to establish the cause of the breach, the effectiveness of the response and to identify areas that require improvement.

Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

Data Theft

It is a crime under the Data Protection Act to steal personal data, and could result in a fine and prosecution. If you suspect data theft has occurred, the Technical Director at Korero should be made aware as soon as possible.

Any abuse of confidential information in any way by a Korero employee will result in the Company implementing its disciplinary procedures and may result in the instant dismissal of that employee.

Where data theft occurs, Korero is required to inform clients and possibly the Information Commissioner's Office, who regulate compliance with the Data Protection Act 2018.

Data Subject Requests

Any data subject requests should follow this procedure:

1. Acknowledge the request: Notify the requester that we have received their request within 1 working day

2. Receive and identify the request: Once a request is received by the Support Team, we should identify the data subject and the request made by the data subject.

3. Verify the identity of the requester: We must verify the identity of the requester before any action can be taken. This needs to involve our most senior contact for the relevant Talent Toolbox client (usually a HR Director or similar). No further action can be taken without the notification and consent from this contact (or from a contact they've delegated it to, with a provable trace of the delegation). It is the client's responsibility to verify the identity of the data subject. This can be achieved through various means such as requesting the requester to provide a valid identity document such as a passport or driver's license, but this is down to the client to handle.

4. Review the request: Next we must review the request and ensure that it is in compliance with relevant data protection regulations. We should check if there is any missing detail that needs to be added to the request, and whether our key contact has any objections to the request before proceeding.

5. Respond to the request: We must respond to the request within the legal timeframe required by data protection regulations. The response will include a copy of the data held (where applicable) and any additional information required to meet the request.

6. Provide access to the data: We must provide access to the data requested by the data subject. This can be done either by providing the data in an electronic format via an pre-agreed transfer method, e.g. via a secure download link.

7. Amend or delete the data: We should act accordingly based on the request made by the data subject. This may include amending or deleting certain data, subject to the regulation requirement.

8. Ensure compliance with data protection regulations: We must ensure that all actions taken related to the data subject's rights are in compliance with data protection regulations.

9. Document the request and actions: We should document the entire process and actions taken. This will help to demonstrate compliance in case of an audit.

10. Report any breaches: If there has been any breach, potential or actual, we must report the incident to our client in line with our breach process, along with the relevant authorities in compliance with data protection regulations.

Kōrero

Penetration Testing

Penetration testing consists of testing an application's security using the same methods and techniques that attackers would use. Feedback from this testing is used to develop and improve security of Talent Toolbox.

Black-box testing is performed to ensure the application and all client data is secure. This testing is performed on a scheduled basis, with extra testing performed when a significant change or addition is made to Talent Toolbox.

Information Risk Management Plc are the current providers of penetration testing for Talent Toolbox. Well-respected within their field, IRM are an international information security consultancy with over 20 years' experience working with large enterprises.

Appendices

Appendix A: Network Diagram

(Also available at:
https://raw.githubusercontent.com/TalentToolbox/Documentation/master/Disaster-Recovery/Network-Diagram.jpg)