

TalentToolbox

The Innovative People Solution

Software-as-a-Service

Business Continuity,
Security & Data Policies



Powering People Performance

Contents

- Version History 3
- Introduction 4
- Business Continuity Management..... 5
 - Disaster Recovery..... 5
 - Procedures and Responsibilities 5
 - Example Scenario: Complete Loss of Primary Datacentre Facility..... 6
 - Testing Procedure 7
 - Backup Policies..... 8
 - Source Code 8
 - Web Application Hosting Environments..... 8
 - Databases 8
- Security Plan 10
 - Data Breaches 10
 - Introduction 10
 - What is a breach? 10
 - Reporting of the breach 10
 - Investigation and Risk Assessment..... 10
 - Containment and Recovery 10
 - Notification..... 11
 - Review..... 11
 - Data Theft..... 11
 - Privacy Issues 11
 - Data Protection 11
- Appendices..... 12
 - Appendix A: Network Diagram..... 12

Powering People Performance

Version History

| Version | Date | Comment(s) |
|---------|------------|------------------|
| 1.0 | 30/09/2014 | Initial creation |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Powering People Performance

Introduction

ICT continuity management supports the overall business continuity management (BCM) process for clients of Purple Cubed's software-as-a-service products (or SAAS, referred to hereafter as "services"). BCM seeks to ensure that Purple Cubed's services are protected from disruption and that Purple Cubed 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 Purple Cubed and its clients.

Due to 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 Purple Cubed, but without going to the levels required by a mission critical service.

Powering People Performance

Business Continuity Management

In the event of an severe unplanned service disruption, whereby Talent Toolbox is expected to be unavailable for a significant period of time (over 1 hour), responsibilities and procedures are defined to ensure the right people are involved to enable Purple Cubed 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 there's no simple resolution
- Notify the Operations Director and Operations Managers about the disruption so they can keep their clients up-to-date
- Coordinate diagnosis of the root cause of the disruption with the Development Team, providing an estimated time to the Operations Team for when normal service will resume
- Liaise with the hosting provider if the root cause concerns hosting
- Provide guidance to the Development Team where necessary to ensure a resolution is found as quickly as possible
- Notify the Operations 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
- Notify the Operations 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 the effectiveness of it and identify any areas that could be improved

Development 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 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

Operations 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 before releasing to clients

All of Purple Cubed

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

Powering People Performance

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 Operations 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 Operations 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 development team members will check the status page 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 Operations 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 nightly 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

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

Review

The Response Team gather together, lead 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.

Powering People Performance

Testing Procedure

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

Purple Cubed 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 |

Powering People Performance

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.

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, Purple Cubed 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.

Powering People Performance

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 Purple Cubed to test restoring of database backups.

Powering People Performance

Security Plan

Data Breaches

Introduction

Talent Toolbox holds data about its clients and their employees. This includes a small amount of personal data, such as names, dates of birth, contact details.

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, 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
- Loss of data or equipment through fire or flood, for instance
- Hacking attack
- Where information is obtained by deceiving an employee of Purple Cubed

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 instigate a Response Team, who will be responsible for investigating data breaches. An investigation will be started within 24 hours of the breach being discovered, where possible.

The investigation will establish the nature of the breach, the type of data involved, whether the data is personal data relating to individuals, 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 isolating a compromised section of the system or temporarily shutting it down completely.

Powering People Performance

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.

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 a decision to inform any external organisation, such as the police or other appropriate regulatory body.

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

Notice of the breach will be made to affected individuals to enable them to take steps to protect themselves. This notice will include a description of the breach and the steps taken to mitigate the risks, and will be undertaken by the Response Team.

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

ASK CLAIRE

Privacy Issues

ASK CLAIRE

Data Protection

ASK CLAIRE

Powering People Performance

Appendices

Appendix A: Network Diagram

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

