TRAC2 5.2.4

5.2.4 - The repository shall have suitable written disaster preparedness and recovery plan(s), including at least one off-site backup of all preserved information together with an off-site copy of the recovery plan(s).

Introduction

In collaboration with the University of Toronto Libraries' (UTL) administration and the Libraries' Information Technology Services (ITS) department, SP has already implemented a variety of disaster preparedness and minimization strategies for a wide variety of threats. The repository's Risk Analysis and Management Strategies document describes the full range of risk management strategies. The core strategy is the repository's Backup Plan. In the event of a disaster that leads to data corruption or loss, SP staff will work with ITS to restore information from backup copies.

SP is developing a written Disaster Recovery Plan that will reflect its operational relationship with UTL and ITS. The policies and procedures described in the Disaster Recovery Plan will reflect some of the threats analyzed in the repository's Risk Analysis and Management Strategies document. However, the Disaster Recovery Plan will focus on systematic procedures for managing large-scale data corruption or loss. The plan will provide step-by-step instructions for addressing and resolving episodes of data corruption or loss (or situations where data corruption or loss is possible but not certain). Steps will include assessing the extent of any damage, retrieving content from backup copies, validating the authenticity and integrity of information, and restoring full dissemination services. The plan will describe emergency contacts, staff roles and responsibilities, communication priorities, and data recovery procedures. Part of the planning process involves identifying a suitable off-site storage location for copies of the plan.

Responsibility

Digital Preservation Policy Librarian

Systems Administrator

Potential Risks

The chief risks associated with a disaster recovery plan are (1) failure to review and update the plan in a timely and consistent manner, (2) failure to inform staff about the plan, and (3) failure to train staff in disaster recovery procedures. To minimize the first risk, SP has monitoring commitments in place (see Monitoring Commitments below). With respect to the second and third risks, SP has a documented Backup Plan and a formal agreement with ITS for data recovery. The repository will implement formal communication and training processes as a part of its Disaster Recovery Plan.

Monitoring Commitments

The repository will assess its Disaster Recovery Plan on a regular basis, according to the Review Cycle for Documentation Policy, or whenever there are major changes to its operating environment such as hardware refreshment or significant staffing level changes. In addition, SP will review the plan after any disaster during which staff consulted the plan or any episode of large-scale data corruption or loss.

Future Plans

The Disaster Recovery Plan is currently in development.

Relevant Documents

1. Disaster Recovery Plan
2. Backup Plan
3. Risk Analysis and Management Strategies
4. Review Cycle for Documentation Policy