The Glasgow School of Art

GSA IT Backup and Recovery Policy

September 2016

Policy Control

<table>
<thead>
<tr>
<th>Title</th>
<th>GSA IT Backup and Recovery Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Approved</td>
<td>Sep 2016</td>
</tr>
<tr>
<td>Approving Bodies</td>
<td>Executive Group</td>
</tr>
<tr>
<td>Implementation Date</td>
<td>Sep 2016</td>
</tr>
<tr>
<td>Supersedes</td>
<td>N/A</td>
</tr>
<tr>
<td>Supporting Policy</td>
<td>Communications &amp; Information Technology Security Policy</td>
</tr>
<tr>
<td>Review Date</td>
<td>Sep 2019</td>
</tr>
<tr>
<td>Author</td>
<td>Sid Meldrum, Network Manager</td>
</tr>
<tr>
<td>Date of Impact Assessment</td>
<td>tbc</td>
</tr>
<tr>
<td>Benchmarking</td>
<td>Glasgow Caledonian University</td>
</tr>
<tr>
<td></td>
<td>University of Strathclyde</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

GSA is a centre of knowledge, learning and research and, in common with other institutions within the HE sector, is now heavily reliant on the use of computing and network technology to support, manage and distribute the information that is a key asset for GSA.

GSA’s ability to exploit and gain advantage from its information base enables it to maintain and improve its reputation and meet its strategic, business and professional goals, as well as conducting its day-to-day operations effectively. The information used by GSA is one of its major assets and, without it, the School would have difficulty providing a service to our students and other third parties with whom we have relationships.

The information systems (hardware and software) supporting the institutions bussiness are varied and represent a sizeable investment that must be protected. The value of information stored should not be underestimated and in many cases data may not be easily reproduced.
It is vital that GSA adopt consistent policies, appropriate and cost effective strategies and good practice to ensure that all electronic information resources on which GSA depends, and the IT infrastructure on which they reside, are protected against loss of data or corruption.

This policy will support and strengthen the implementation of GSA’s Information Systems and Information Technology Strategies.

2. OBJECTIVES

- Maintain business continuity within the institution in the event of disaster.
- To protect the institution against the loss of data in the event of other minor incidents which may lead to the loss of data (e.g. data corruption).
- To further develop and maintain a high level of resilience over the institutions Information systems.

3. SCOPE

- This policy applies throughout GSA. It applies to all staff and students within GSA who create, manage or use data that is owned, managed or stored by GSA. The policy also applies to anyone, including third parties, who manage or have responsibility for systems or data stored on systems within GSA.
- Additionally, in recognition of movement within the institution to use cloud base services the policy applies to all those within the institution having responsibility for management and/or co-ordination of services which may be provided externally by a third party in a cloud based environment.
- The scope of the individual supporting documents is specified within the list of those documents.

4. PRINCIPLES

The principles of this policy are:

- The key purpose of this policy is to define minimum controls required for the backup of GSA IT systems and data to meet the institutions objectives.
- To safeguard against the loss of data that may occur due to hardware or software failure, physical disaster or human error.
- To have a risk aware approach that identifies and addresses unacceptable risks, while maintaining a knowledgeable and reasoned acceptance of other risks

Responsibilities

- Formulation and review of the GSA IT Backup & Recovery Policy is the responsibility of the Network Manager, reporting to the Director of IT. The Director of IT is responsible and accountable for ensuring that objectives for GSA Backup and Recovery are achieved. Approval of the policy lies with the GSA Executive Group.
• The institution has responsibility to ensure adequate resourcing to maintain and develop this Policy, based on advice from the Director of IT.

• The GSA IT network team are currently responsible for the management of all GSA IT department backup systems and associated documents relating to such backup systems.

• Data custodians are responsible for ensuring that appropriate backup schedules are arranged with The GSA IT department. Additionally GSA staff with responsibility for production and management of data must ensure important institutional data under their control is included in the GSA Backup plan.

• All users within GSA have responsibility for the management of institutional data under their control. Staff should ensure that all valuable data both organisational and personal is stored on a recognised GSA data server. End users should not store data on personal computers and/or external devices such as removable hard drives which are not protected by backup.

• Staff having supervisory responsibility are required to coach and encourage best practice amongst their supervised staff or students.

• Data backups are not intended to serve as archived copies of data or to meet requirements relating to institutions record keeping.

• This policy is applicable to all staff within the institution (including its Schools and Professional Support areas) and third parties who process and/or store Institutional data.

• The GSA backup and recovery process is applied to all data held within the Institutions recognised data centres. Responsibility for backup of data held on any computer or device out with these recognised locations, regardless of ownership, falls entirely on the owner/user of the device.

• Specifications relating to systems and application servers must include a section detailing System, data and application backup requirement.

Definitions

IT (Information Technology) is the GSA department responsible for the provision of backup and recovery services for data held in the Institutional Data Centre.

GSA Data centres are defined as the key physical locations within the institution which hold the institutional Information systems and provide the institutions information technology services. Currently these centres are in the Bourdon, Reid and Digital Design buildings. Additionally In 2017 Stow will provide a new primary data centre facility.

Granularity is the frequency with which data is backed up. Data that is present for less than this time period may not be captured by the backup process and hence may not be recoverable.

Retention is the length of time a backup is kept. At the end of the retention period the backup is deleted.

Structure

The GSA IT Backup and Recovery Policy consists of this high-level overarching document and a number of supporting documents.
5. **POLICY**

1. **Backup and Recovery Policy**

GSA requires that all institutional data is backed up according to the following policy:

1.1 Complete records must be kept as to what data and systems are being backed up.

1.2 All Schedules for backup must be recorded and maintained.

1.3 All Backup media must be clearly labelled.

1.4 Where tape media is placed or held within data centre tape library tapes must be bar coded.

1.5 Backups should not be stored in the same building as the live data or system. GSA should strive to ensure geographically diverse locations between the primary data/systems and their backup.

1.6 Data and system recovery processes must be tested frequently. The maximum period between tests should not exceed three months. Testing of recovery procedures must be undertaken to ensure that backup data can be used to re-instate data in an emergency or disaster situation. A record of backup testing must be maintained. Where a natural data or system recovery is required this can be used to contribute towards the testing process, provided details of the recovery are recorded.

1.7 Recovery procedures for the restoration of data must be maintained and up to date.

1.8 Records pertaining to points 1.1 – 1.6 above must be managed and retained for audit purposes.

1.9 All users must ensure that important organisational and personal data is stored on a recognised GSA data server and not on personal computers or workstations as these are not backed up.

2. **Backup Schedules**

GSA requires that the institutions systems and data are backed up in line with the following schedules:

2.1 **Backup of data (Staff/Student data, commercial data, and application data).**

- Every day a data backup is taken and retained for 14 days.

- Backup cycles are 7 days.

- The first Backup in each cycle must be a full Backup.

- For subsequent backups in each cycle backup type (Full, Differential, or Incremental) must be defined and recorded.

- Data created or deleted less than 24 hours between backups or data deleted more than 14 days before the backup was created cannot be recovered.
The following schedule provides for data to be restored with at most one working days data missing.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Granularity</th>
<th>Retention Period</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application &amp; Databases</td>
<td>1</td>
<td>14</td>
<td>2nd data centre</td>
</tr>
<tr>
<td>Staff/Student User Documents and files</td>
<td>1</td>
<td>14</td>
<td>2nd data centre</td>
</tr>
<tr>
<td>Commercial Data</td>
<td>1</td>
<td>28</td>
<td>2nd data centre</td>
</tr>
</tbody>
</table>

2.2 Backup of Systems

Backup for GSA systems is required to protect the organisations vital business and operational systems. System backup must be provided for all infrastructure, business and data systems to ensure that in the event of any significant disaster, such as loss of data centre or system, business critical systems can be restored within a reasonable time frame.

To facilitate quick recovery of systems GSA must maintain the following types of backup:

1. Backup copies of systems in the form of images which can be restored to any location or platform.
2. Replicate all virtual key systems adhering to this Backup Policy, particularly with regard to location.
3. Ensure additional backup of data and system configurations are in place for all systems.

2.2.1 Backup of Systems (hardware platform)

- All system image backups must be full backup.
- Changes to systems less than 7 days between backups must be captured daily using configuration backup.
- Additional database backup process must be applied to all systems holding databases.

The following table provides the backup schedule for imaging of GSA Systems. This schedule dictates the frequency for full system images based directly on hardware platforms (not virtualised).

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Granularity</th>
<th>Backup Retention Period</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure Systems</td>
<td>7*</td>
<td>14</td>
<td>2nd data centre</td>
</tr>
<tr>
<td>Application Systems</td>
<td>7*</td>
<td>14</td>
<td>2nd data centre</td>
</tr>
<tr>
<td>Commercial Systems</td>
<td>1*</td>
<td>14</td>
<td>2nd data centre</td>
</tr>
</tbody>
</table>

2.2.2 Backup of Systems (Virtual platform)

With a few exceptions GSAs infrastructure and application systems are homed in a virtual environment using VMware ESXi. In order for GSA to maximise benefit from this type of deployment these systems must be replicated frequently to provide an additional level of resilience in event of a hardware failure or local disaster. The schedule below indicates frequency for replication of all virtual servers. This replication must
observe backup policy by ensuring that replicas are housed in a different physical location to the original virtual server.

- All system replication backups must be full backup.
- Changes to systems less than 7 days between backups must be captured on a daily using additional configuration backup.
- Additional database backup process must be applied to all systems holding databases.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Granularity (days)</th>
<th>Backup Retention Period</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Duration (days)between backed ups</td>
<td>Duration backup retained(days)</td>
<td></td>
</tr>
<tr>
<td>Core Infrastructure Systems (Domain Controllers)</td>
<td>1*</td>
<td>Replica over written on backup.</td>
<td>2nd data centre</td>
</tr>
<tr>
<td>Infrastructure Systems</td>
<td>7*</td>
<td>Replica over written on backup.</td>
<td>2nd data centre</td>
</tr>
<tr>
<td>Application Systems</td>
<td>7*</td>
<td>Replica over written on backup.</td>
<td>2nd data centre</td>
</tr>
<tr>
<td>Commercial Systems</td>
<td>1*</td>
<td>Replica over written on backup.</td>
<td>2nd data centre</td>
</tr>
</tbody>
</table>

(*Additional backup methods must be used – System Backup [image]+ configuration).

2.2.3 Backup of System configurations

Replication of GSA servers enhances recovery of systems. In many instances the replication process may not be frequent enough to ensure full recovery of status or configuration of a system in the event of recovery.

In order to mitigate the risk, where this exists, configuration backup must be taken at more regular frequency than full replication or system image.

- All system configuration backups must be full backup.
- Changes to systems less than granularity period cannot be restored.

The following table outlines the schedule for system configuration backups. Details of which data should be backed up must be detailed in the GSA Backup Procedure documentation.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Granularity</th>
<th>Backup Retention Period</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Duration (Hours)between backed ups</td>
<td>Duration backup retained(Days)</td>
<td></td>
</tr>
<tr>
<td>Domain Controllers</td>
<td>24*</td>
<td>14</td>
<td>2nd data centre</td>
</tr>
<tr>
<td>Print Account System</td>
<td>1*</td>
<td>14</td>
<td>2nd data centre</td>
</tr>
<tr>
<td>Application Servers</td>
<td>24*</td>
<td>14</td>
<td>2nd data centre</td>
</tr>
</tbody>
</table>
Implementation of GSA system protection using both backup and replication

3. Data Recovery

This section of the policy document outlines the policy for recovery of data relating to GSA Backup.

1. Request to recover data or systems should be submitted to the IT Service Desk. Requests must be made at earliest possible time following loss of data or system.

2. The GSA IT department cannot accept responsibility for delay by a member department or individual to register requests for data or system restoration.

3. Data restoration from backup is subject to the retention and granularity periods defined within this backup policy (Backup schedules section 2).

4. Backup policy recovery schedules. Where requests to recovery data from backup are processed the GSA IT department must endeavour to process such request as soon as possible following receipt. The following table summarises recovery schedules for types of backup carried out by the GSA IT department.
GSA Backup and Recovery Policy

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Recovery Period (Hours from request receipt)</th>
<th>Type of Recovery</th>
<th>Potential data loss (The period of potential difference [hours] between loss of data &amp; last backup)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Data files stored on GSA data servers (Not exceeding 5GB).</td>
<td>24 Hours</td>
<td>Permanent recovery to original data location.</td>
<td>24 Hours</td>
</tr>
<tr>
<td>Personal Data files stored on GSA data server (exceeding 5GB).</td>
<td>48 Hours</td>
<td>Permanent recovery to original data location.</td>
<td>24 hours</td>
</tr>
<tr>
<td>Application Data bases</td>
<td>48 Hours</td>
<td>Permanent recovery to original data location.</td>
<td>24 Hours</td>
</tr>
<tr>
<td>Printing Accounting System</td>
<td>3 Hours</td>
<td>Initial recovery using system replica. Later Scheduled Permanent recovery to original data location.</td>
<td>2 Hours</td>
</tr>
<tr>
<td>Departmental and Application Servers*</td>
<td>3 Hours</td>
<td>Initial recovery using system replica. Later Scheduled Permanent recovery to original data location.</td>
<td>No data loss anticipated.</td>
</tr>
<tr>
<td>Infrastructure servers</td>
<td>3 Hours</td>
<td>Initial recovery using system replica. Later Scheduled Permanent recovery to original data location.</td>
<td>12 Hours</td>
</tr>
</tbody>
</table>

(* Server holds databases schedules for Application databases must be applied.)

6. POLICY AWARENESS

An electronic copy will be made available on the GSA website.

7. IT DATA RECOVERY INCIDENT LOG

A record will be maintained within the IT Service Desk software in which all IT Data recovery Incidents will be recorded along with details of any action taken. All staff (from all Departments) will have a responsibility to log with the IT Service Desk any incidents that relate to recovery of Data.

8. RELATED POLICIES AND DOCUMENTS

The following is a brief summary of documents associated with this backup policy. Full copies of these can be obtained from the GSA website.

GSA Policy for Staff Electronic File Backup
This policy outlines criteria for categorising importance of data handled by GSA staff. The policy outlines the process for ensuring backup of all important business data.

GSA Staff Acceptable IT Use Policy
The reason for this policy is to ensure the proper use of all of GSA’s computing and network facilities.
**GSA IT Staff Backup Procedures**
This document is held by the GSA IT department and details current procedures and processes relating to GSA backup.

**GSA IT Staff Backup Schedules**
This document is held by the GSA IT department and details current schedules applied to backup for all GSA systems and data. In addition to schedules, the document acts as a single reference point and summary for all GSA backup indicating what data on which systems is backed up.