Policy Title – BACKUP & RESTORE POLICY

Table of Contents

Policy Summary

The Police and Crime Commissioner (PCC) and Chief Constable (CC) for Gloucestershire are responsible for the Confidentiality, Integrity, and Availability of all policing and business related data stored on systems owned by Gloucestershire Constabulary.

The PCC and CC for Gloucestershire have an obligation under UK GDPR and the College of Policing Approved Professional Practice for Information Assurance to ensure that information assets and service configuration backups are completed on a regular basis and available for restoration in the event of disaster recovery. Effective implementation of this policy will limit data loss.

This policy document defines the obligations placed upon Information Communication Technology (ICT) staff, business units and management. It outlines the underlying requirements for backup and restore requirements and is supported by the backup and restore procedure.

Policy should enable consistent and effective decision-making. Where operational or managerial circumstances require any decision making that would adversely affect adherence to the policy or procedure, in line with the 'Statement of Intent' of the constabulary and the police service 'Code of Ethics', if an officer/ police staff member believes that they need to make a decision that steps outside of policy and procedure they should do so, provided that:

- The officer/ police staff member raises the matter at the earliest opportunity (and ideally before any such decision is made) with their line manager declaring their intended (or actual) course of action if notification is made after the decision is taken,
- Produces, in a timely manner, a signed and dated written explanation of why it is/ was deemed necessary to step outside of policy and procedure, and
- Maintain an adequate record of this written rationale for audit purposes appropriate to the circumstances/ contravention.

Key Principles

Gloucestershire Constabulary policy statements regarding backup and restore are as outlined below;

- Where strategically identified, Gloucestershire Constabulary information assets managed by the ICT department will be backed up (or replicated) on a regular basis. This will be to both onsite and offsite storage, and have restore ability.
- Where strategically identified, Gloucestershire Constabulary services managed by the ICT department will be backed up (or replicated) on a regular basis. This will be to both onsite and offsite storage, and have restore ability.

- Depending on the location of the service/data the offsite storage locations are the Constabulary's data centres.
- The backup retention period is set to the business requirement for the system or asset:
    - File server and email 30 days of restore points.
    - Front end applications instructed by Service Manager of 7 versions.
    - Production Online Transaction Processing (OLTP) databases - 7 days (default) of restore points.
    - Online Analytical Processing (OLAP) and non-production databases - 3 days (default) of restore points.
- Backup schedules are determined by completion of a Business Impact Assessment by the business area owners. ICT will set the backup schedules as required. BIA's are being created in September 2021 for all business owners and a full review of the backup strategy is then required.
- Restore testing will be performed as part of the Disaster Recovery test planning.
- ICT will be responsible for managing the backup schedules (as defined by business area owners) and will follow internal incident management procedures to communicate and correct any incidents impacting the backup and restore service.

Compliance

This policy has been prepared taking account of prevailing legislation. New legislative requirements or changes in current legislation may necessitate a review of this policy document.

Our policies are intended to promote equality, eliminate unlawful discrimination and actively promote good relationships regardless of: age, disability, gender, race or ethnicity, religion and Belief and sexual orientation.

This policy has been impact assessed using the Equalities Impact Assessment Template. By building equality considerations into our policy-making process, we have been able to identify any actual or potential inequalities and reduced them as much as possible, by applying the policy differently or looking for alternatives.

Relevant Legislation / Regulations

Regulatory and Legislative requirements applicable to this policy:

- Data Protection Act 2018
- UK GDPR
- Computer Misuse Act 1990
- College of Policing Approved Professional Practice for Information Assurance

Consultation

This policy has been created to meet the above requirements and the following people have been consulted: -

- Head of Digital and Data Services
- Technical Infrastructure Manager
- Senior Security Analyst
- Head Governance and Compliance
- Force Information Security Officer
- ICT Service Manager Group (all teams)

Procedure

Supporting procedures will be produced and are available to relevant ICT staff.

Identification, Monitoring and Review

Security Marking:	**NOT PROTECTIVELY MARKED**

Document Title: POLICY

Backup and Restore Policy

Type	**URN**	**Strategic Board**	**Author/Reviewer**
Policy	**302**	**IGB**	**Author: ICT Technical Infrastructure manager** **Reviewer: Force Information Security Officer**

Version	**Date**	**Changes (ensure public copy amended and uploaded to external website)**	**Complied with Policy Guidance ✓**
0.1	**19/03/21**	**Creation of draft policy for review**	✓
0.2	**22/03/21**	**Insertion of legislative interdependencies**	
0.3	**25/05/21**	**Update of first draft including legislative requirements and business processes. Removal of GSC protective marking**	
0.4	**14/06/21**	**Update re review following planned BIA completion September 21**	
1.0	**14/06/21**	**V1.0 for circulation to IGB**	

Next Document Review Date: October 2021

EIA	**EIA Sign Off**	**EIA Review**
LOW		
SIA	**SIA Sign Off**	**SIA Review**

This version will be placed on the public domain website

If this version cannot be placed on the public domain website, provide reason and relevant COG authority and FOI version	This policy is suitable for publication under the FOI