Backup and Recovery

Policy Intent and Objectives	The intent of this policy is to protect Paylock information system and asset availability, integrity, and confidentiality by defining requirements for backup and recovery.
Policy Scope	This policy applies to all Paylock information systems.
Exceptions	Exceptions to this policy must be documented and approved following Paylock's Exception Procedures.
Enforcement	Violators of this policy are subject to immediate termination of access, and to disciplinary action, as deemed appropriate by Paylock management. Violators may also be subject to local, state, or federal legal action, depending on the severity of the violation.
Owner	Paul Chiafullo
Approval Date	01 Dec 2021
Related Documents	ISO/IEC 27001/27002:2013 - A12.3

Policy Statements and Guidance	• Documented procedures to monitor the execution of backups, address failures of scheduled backups, and restore backups shall be produced and updated as necessary. • The extent (e.g., full or differential backup) and frequency of backups shall reflect business requirements, the security requirements of the information involved, and the criticality of the information (i.e., to match business continuity requirements). • Copies of backups shall be made to ensure the integrity of recovery can be maintained, and accurate and complete records of the backup copies shall be documented. • Backups shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the primary site. • Backup information shall be given an appropriate level of physical and environmental protection. • Backup media must be encrypted per corporate standards when confidentiality of the data must be insured. • Backup arrangements for individual systems and services shall be regularly tested to ensure that they meet the requirements of business continuity plans. • The retention period for essential business information shall be determined, taking into account any requirement for archive copies to be permanently retained (e.g., litigation hold), regulatory requirements, and defined retention schedules. • Periodic reviews should be conducted, at least annually, to inspect offsite storage facilities to verify retention schedule adherence, and security and environmental controls. • An annual reconciliation review shall take place to ensure all backup media containing critical data is accounted for. • Sensitive backup data shall only be transported via bonded and insured carriers (as approved by @ Syed Haider aul Chiafullo).

Policy Revision History

This policy will be reviewed, at a minimum, on an annual basis or as needed due to legal, regulatory or corporate directives. The review will include approval by senior management of Paylock prior to any changes being made to the policy.

Date of Policy Change	Description of Policy Change	Change Made By

24 Jul 2017	Creation of policy document	@ Syed Haider
03 Jul 2019	Executed policy	@ Syed Haider
12/01/2021	Policy review - no change	Doreen Gossage