Physical and Environmental Security

Policy Intent and Objectives	This policy provides guidance on Paylock physical and environmental security controls that should be implemented for protection against unauthorized access, damage, or interference to business facilities and information resources.
Policy Scope	This policy applies to all Paylock sites, facilities, personnel, consultants, contractors, vendors, or any other personnel with access to Paylock resources.
Policy Exceptions	Exceptions to this policy must be documented and approved following Paylock's Exception Procedures.
Policy Enforcement	Violators of this policy are subject to immediate termination of access, and to disciplinary action, as deemed appropriate by Paylock's 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	12/01/2021
Related	ISO/IEC 27001/27002:2013 – A.11 Access Control Policy Delivery/Loading Area Security Procedure Equipment Disposal Procedure Equipment Maintenance Procedure Records Retention Standard Removal of Assets Procedure Systems Clock Synchronization Standard Visitor Management Procedure

Policy Statements and Guidance	• Security perimeters shall be implemented to protect areas that contain either sensitive or critical information or information processing facilities. The security measures should be commensurate with the value of the assets contained within the perimeter and an associated formal risk assessment. • All physical security systems, and physical ingress and egress areas (including fire exit doors), must comply with applicable laws and regulations such as, but not limited to, building codes and fire prevention codes. • An occupied reception area, or other means to control physical access to Paylock sites or facilities, shall be in place. • Access to Paylock sites or facilities shall be restricted to authorized personnel only. • Access to areas where confidential or sensitive information is processed, stored, or transmitted shall have access restricted to authorized Paylock personnel only, using appropriate access controls. • The use of photographic, video, audio, or other recording equipment, such as cameras in mobile devices, shall not be permitted in areas containing sensitive or confidential information or processes, unless an exception has been granted through the Paylock Exception Procedure. • Paylock sites or facilities shall be configured in such a manner that confidential, sensitive, or proprietary information and/or activities cannot be observed by non- Paylock employees. • Physical access within Paylock sites or facilities shall be securely managed and maintained via electronic access records. Physical logbooks shall be securely maintained and managed where electronic access records are not possible or practical. • Procedures and/or standards shall be documented and followed for the security of: • Delivery and loading areas at Paylock sites and facilities to ensure a secure perimeter. • Utility providers supporting the Paylock infrastructure. • Equipment maintenance. • Removal of assets. • Off-premises Paylock equipment. • Redeployment or disposal of equipment. • Security considerations for a new site or facility, or modified site or facility, construction. • Visitors of Paylock sites or facilities. • Creation, modification, or termination of physical access to Paylock sites or facilities.

Policy Statements and Guidance (continued)	• Video surveillance of Paylock sites and facilities shall be securely managed and controlled. • Video recording system time clocks should be synchronized, per the Systems Clock Synchronization Standard, with other access control mechanisms, such as badge readers, to provide a complete and accurate trail of someone's activities. • A retention schedule for video recordings shall be kept for a period of time in accordance with Paylock's corporate, legal, and regulatory requirements. The retention schedule for the video recordings should be consistent with the policies Logging and Monitoring, Backup And Recovery, and Information Classification. • Video recordings shall be tested on a regular basis to ensure they are adhering to their retention schedule, and are available in the event of investigations or for auditing purposes. • Identification badges should be worn by contractors, third-party users and visitors, and visible at all times while in Paylock facilities. Visitors must be escorted at all times by authorized badged personnel.

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
12/01/2021	Policy review - no change	Doreen Gossage