Access Control

Policy Intent and Objectives	The intent of this policy is to ensure that access to Paylock's information assets and systems is restricted to those who require it to perform their business functions. This policy will also ensure that the administration of user access to Paylock's information assets and systems applies the principles of information classification, least privilege, need-to-know, and role-based access.
Policy Scope	This policy applies to all Paylock personnel, consultants, contractors, vendors, or any other person 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.9 Confidentiality Agreement Information Classification Policy Information Classification Standard Non-Disclosure Agreement Password Standard Supplier Management Policy

Policy Statements and Guidance	• Users shall only be provided with the minimum access required (i.e., least privilege) to the network, network services, and data that they have been specifically authorized to use in order to perform their job function. If administrative privileges are given to a user, an audit trail of administrative access external to the machine is kept. • Each user shall be assigned a unique User ID and password. Requests for shared, generic, and system (e.g., service) accounts shall be documented, including the purpose, and have the appropriate management sign-off. • A formal user access provisioning process shall be implemented to assign, modify, or revoke access rights for all user types to all systems and services. • The access rights of all employees and external parties, including contractors, vendors, consultants, customers and business partners, to information and information processing facilities, shall be removed upon termination of their employment, contract or agreement, or modified upon change. • Accounts that have been inactive for more than 45 days shall be disabled. • Accounts that have been inactive for more than 90 days shall be deleted, document exceptions apply, ie medical leave, military leave etc. • Users shall protect and shall not share secret authentication information. • Users shall not use the same passwords for business and non-business purposes. • Password management systems shall be interactive and shall enforce Paylock's Password Standards. • The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. • Asset owners shall review users' access rights at regular intervals. • Access to program source code shall be restricted the Engineering team as defined in the Source Code policy. • Multi-factor authentication will be implemented as deemed appropriate per Paylock policies, procedures or standards.

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
01-24-2017	Creation of policy document	Jennifer Marston
01-24-2017	Policy executed	Syed Haider
12-01-2021	Policy review - no change	Doreen Gossage