Mobile Devices

Policy Intent and Objectives	To define the policy regarding the use of mobile devices to access Paylock's information environment, resources, and data.
Policy Scope	This policy applies to all Paylock 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.6.2.1 Cryptography Standard Mobile Device Software Standard Mobile Device Tracking Process Password Standards

Policy Statements and Guidance	• A process shall be created to track the use of all mobile devices with access to Paylock data. • Use of mobile devices[1] are permitted in the Paylock environment, provided the following safeguards are in place: • All mobile devices shall be registered and approved for business purposes by the employees' manager. • Employees are expected to exercise due care in the physical protection of mobile devices. • Software on Corporate-provided mobile devices must be approved by IT. • Mobile devices shall be kept up-to-date with the latest available patches and operating systems by the custodian of the device. • Connecting to corporate systems through the mobile device for any reason outside of job responsibilities is prohibited. • Encryption (if available), passwords, passcodes, or biometrics are in place on the mobile device in order to protect the data in the event it is lost or stolen. Passwords should be at least twelve (12) characters in length, contain uppercase and lowercase letters, numbers, and special symbols, do not contain memorable keyboard paths and are not based on personal information. • Multi-Factor Authentication should be turned on. • Paylock reserves the right to remotely lock, erase or disable any mobile device due to theft, loss of the device, termination of employment, or other reasons deemed necessary to protect the interests of Paylock. • Lost or stolen mobile devices used for business purposes must be reported to Information Security immediately. For stolen mobile devices, a police report shall also be filed and supplied to Paylock in a timely manner.

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	Password rules and MFA	Doreen Gossage

1 For the scope of this document, mobile devices refer to smartphones and tablets. Other devices like laptops are out of scope for this policy.