Acceptable Use

Policy Intent and Objectives	The intent of this policy is to outline the acceptable and unacceptable use of information assets/systems at Paylock. These rules are in place to protect our employees, partners, customers, and the Company from risks such as malware, compromise of sensitive information, and non-compliance. Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information assets and/or information systems. It is the responsibility of every user to know and understand this policy, and to conduct their activities accordingly.
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	01 Dec 2021
Related	All Paylock Information Security Policies, Procedures, and Standards Paylock Code Of Conduct

Policy Statements and Guidance	• Users shall comply with federal, state, and local laws, industry regulations, and the Paylock Code of Conduct.
	• Users shall comply with all Paylock policies, standards, and procedures.
	• Access to Paylock information assets or systems is provided for the purpose of Paylock business, and is not intended for personal purposes, other than reasonable and non-confidential communications. Users are responsible for exercising good judgment regarding the protection and security of these assets.
	• Information assets or systems shall not be used:
	  • To create the impression, without authority, that any communication has Paylock's official sanction.
	  • For any illegal or immoral purpose, any political purpose, or any commercial purpose other than official Paylock business.
	  • To cause a disruption to the Paylock's computing environment, such as the introduction of malicious programs into the network (e.g., viruses, worms, Trojan horses, email or logic bombs, etc.).
	• No Paylock personnel, consultants, contractors, vendors, or anyone else with access to Paylock resources shall disable or circumvent any security feature unless the need is clearly defined, documented, and approved by an official of the business.
	• Only Paylock-IT licensed and approved software may be used on a system or by an individual authorized for that software. Users shall comply with all software license and copyright laws. Users shall not copy any copyrighted materials without the express permission of the creator or owner. This includes, but is not limited to, photographs, graphics, copyrighted music, and software.
	• Paylock retains the right, with employee's knowledge, to monitor and review information assets or systems to ensure compliance with applicable policies and guidelines.
	• When using Paylock-provided information assets or systems, users have no right of privacy with respect to information stored in, transmitted through, or associated with, company-issued hardware, software, the Internet, local and wide area networks, or Intranet web sites.
	• Paylock shall employ measures, at its discretion, to prevent the unproductive, inappropriate, or harmful use of information assets or systems.
	• Communications using Paylock's information systems (including, but not limited to, email, web-browsing, instant messaging) that are racially, ethnically, or sexually offensive, or that offensively address someone's age, sexual orientation, religious or political beliefs, national origin, or disability, or are otherwise offensive, disruptive, demeaning, or harassing, are prohibited.
	• Users shall not store sensitive information on their personal workstations (desktop, laptop, or mobile computing device). Customer information is to be stored on the appropriate file or application server, when possible.

Policy Statements and Guidance (continued)	• Users of the Paylock e-mail system shall not automatically or manually forward non-public e-mail to a non-Paylock e-mail account.
	• User access shall be granted to an individual and may not be transferred to or shared with another user.
	• Neither Paylock, nor any representative, will ever authenticate a user by asking for their passwords. This includes their logon account password or any application account the user may use.
	• Users shall not share their passwords or use another user's password, and shall protect their network account from unauthorized use (e.g., activate screen saver lock). Users shall keep their account password secure from others (e.g., not written down).
	• Users shall not provide personal information about, or lists of, Paylock users to parties outside Paylock without appropriate justification and written approval.
	• Supervisors and Managers shall report changes that require the termination or modification of access or user group permissions granted to users that report to them in a timely manner.
	• Users shall report the following to Information Security:
	  • Potential or actual security violations, including the misuse of information assets or systems.
	  • Potential or actual security incidents.
	  • Unusual computer behavior.
	  • Requests by email or phone for their password.
	  • Requests by email or phone for information from an unverified source that is not authorized to that information per the Paylock Information Classification Policy and the Information Classification Standard.
	  • Violations of the CAN-SPAM Act or any other similar state, federal, or international law.
	• Third parties (e.g., service providers, vendors, outside auditors) shall provide evidence of appropriate security compliance before being granted access to Paylock's computing or information assets. Third party or non-employee access shall be granted for a specified time frame and is subject to renewal each year.

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
03 Jul 2019	Updated Policy Statement Guidance	Syed Haider
01 Dec 2021	Policy Review - no change	Doreen Gossage