Wireless Networks

Policy Intent and Objectives	To define the proper use of the wireless network within the Paylock environment.
Policy Scope	This policy applies to all Paylock personnel, consultants, contractors, vendors, or any other human resource with access to the Paylock environment.
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	12/01/2021
Related Documents	Wireless Network Standard Acceptable Use Network Security

Policy Statements and Guidance	• All vendor default settings must be changed prior to introducing any wireless technologies, including but not limited to, default wireless encryption keys, passwords, and SNMP community strings. • There shall be logical, secure segregation between the Paylock wireless production network and the wireless Guest network. The configuration of these networks shall be such that it is not possible to access one network from the other. • Only approved IT personnel can purchase, configure, and install wireless access points. • Wireless network encryption shall follow the Paylock Cryptography Policy and Cryptography Standard. • Firmware levels for wireless access points in the Paylock environment shall be maintained at current levels. • Rogue access point detection shall be performed through an ongoing monitoring solution. Identified rogue access points emanating from within the Paylock environment shall be investigated, and the results shared with management for further potential disciplinary action. • Paylock assets (e.g., laptops) should not be permitted to use the wireless Guest network. • Wireless networks shall use an authentication mechanism, as defined in the Paylock Wireless Network Standard. The authentication must utilize authentication credentials that are specific to each wireless device or authorized user. The credentials should not be shared. • Pre-Shared Keys (PSKs) for wireless networks are allowed to be used as an exception, the keys must be changed whenever anyone with knowledge of the keys leaves Paylock, or changes positions to where knowledge of the keys is no longer necessary. • Access to the wireless network should be limited only to the designated group of users that need to access the wireless network for legitimate business reasons. • Paylock employees who are hosting guests are to ensure that guests do not use the Internet connectivity in an inappropriate 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	Policy Review - no change	Doreen Gossage
