# Communications Security

| | |
|---|---|
| **Policy Intent and Objectives** | The intent of this policy is to ensure that Paylock communications are properly secured from unauthorized access or disclosure. |
| **Policy Scope** | This policy applies to all Paylock personnel, consultants, contractors, vendors, or any other personnel with access to Paylock resources. |
| **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'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 Documents** | ISO/IEC 27001/27002:2013 – A.13<br><br>Access Control Policy<br><br>Information Classification Policy<br><br>Information Classification Standard<br><br>Physical and Environmental Security Policy |

| | |
|---|---|
| **Policy Statements and Guidance** | • Networks shall be managed and controlled to protect information in systems and applications with consideration for the following:<br>  • Protecting communications (e.g., encryption) based on the Information Classification Policy and the Information Classification Standard.<br>  • Restricting physical and logical access based on Paylock's Access Control Policy, and the Physical and Environmental Policy.<br>  • Allowing only authorized devices to be connected.<br>  • Logging and monitoring based on Paylock's Logging and Monitoring policy.<br>• Production Networks shall be designed to segregate (i.e., segment and filter) groups of information services, users, and systems based on their associated risk profile.<br>• An approved list of communications facilities (e.g., email, SFTP) shall be defined and communicated.<br>• Formal procedures and controls (e.g., encryption) shall be in place to protect the transfer of information through all communication facilities (e.g., electronic messaging, telephony) based on the Paylock Information Classification Policy and the Information Classification Standard.<br>• The use of any encryption software must be validated and approved by Information Security.<br>• IT Management shall designate one or more members of the Information Security team responsible for all system activities regarding encryption. Employees responsible for encryption should review local encryption laws as they pertain to Paylock's deployment and use of encryption technologies.<br>• Legal and Compliance shall be consulted any time that restricted encryption products are being considered for deployment outside of the United States.<br>• Security mechanisms, service levels, and management requirements of all network services shall be identified and included in network services agreements for in-house and outsourced providers.<br>• Contractual agreements shall address the secure transfer of business information between Paylock and external parties.<br>• Requirements for confidentiality or non-disclosure agreements reflecting Paylock's expectations for the protection of information shall be identified, regularly reviewed, and documented. |

| | |
|---|---|
| **Policy Statements and Guidance**<br><br>**(continued)** | • Based on roles and responsibilities within Paylock, it may be necessary to grant employees the ability to use electronic messaging, such as email or Instant Messaging (IM). If this is the case the following rules apply:<br><br>• All communications transmitted, received, or archived via the Company's system are the property of Paylock.<br>• Employees have no reasonable expectation of privacy when using Paylock's systems.<br>• Paylock reserves the right to monitor, access, and disclose all employee communications, from Paylock owned systems and devices.<br>• Users may not share confidential, sensitive, or proprietary information via electronic messaging.<br>• Paylock employees must treat electronic messages as business records, as they may be used as evidence in audits, litigation, and investigations.<br>• All communication shall be in accordance with the refer to the "Paylockian Code of Conduct" |

| | |
|---|---|
| **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 | Jennifer Marston |
| 12/01/2021 | Policy review - no change | Doreen Gossage |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |