Information Security Policy

# Wireless Communication Policy:

## Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

## Purpose

The purpose of this policy is to secure and protect the information assets owned by PXL. PXL provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. PXL grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.   
This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to PXL network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a PXL network.

## Scope

All employees, contractors, consultants, temporary and other workers at PXL, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of PXL must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a PXL network or reside on a PXL site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

## Policy

General Requirements  
All wireless infrastructure devices that reside at a PXL site and connect to a PXL network, or provide access to information classified as PXL Confidential, or above must:   
• Abide by the standards specified in the Wireless Communication Standard.   
• Be installed, supported, and maintained by an approved support team.   
• Use PXL approved authentication protocols and infrastructure.   
• Use PXL approved encryption protocols.   
• Maintain a hardware address (MAC address) that can be registered and tracked.   
• Not interfere with wireless access deployments maintained by other support organizations.

### Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to PXL Confidential or above, must adhere to section 4.1 above. Lab and isolated wireless devices that do not provide general network connectivity to the PXL network must:   
• Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the Lab Security Policy.   
• Not interfere with wireless access deployments maintained by other support organizations.

# Remote Access Policy

## Overview

Remote access to our corporate network is essential to maintain our Team’s productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Hypergolic Reactions, LLC policy, we must mitigate these external risks the best of our ability.

## Purpose

The purpose of this policy is to define rules and requirements for connecting to PXL's network from any host. These rules and requirements are designed to minimize the potential exposure to PXL from damages which may result from unauthorized use of PXL resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical PXL internal systems, and fines or other financial liabilities incurred as a result of those losses.

## Scope

This policy applies to all PXL employees, contractors, vendors and agents with a -owned or personally PXL-owned computer or workstation used to connect to the PXL network. This policy applies to remote access connections used to do work on behalf of PXL, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to PXL networks.

## Policy

It is the responsibility of PXL employees, contractors, vendors and agents with remote access privileges to PXL's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to PXL.

General access to the Internet for recreational use through the PXL network is strictly limited to PXL employees, contractors, vendors and agents (hereafter referred to as “Authorized Users”). When accessing the PXL network from a personal computer, Authorized Users are responsible for preventing access to any PXL computer resources or data by non-Authorized Users. Performance of illegal activities through the PXL network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User’s access. For further information and definitions, see the Acceptable Use Policy.

Authorized Users will not use PXL networks to access the Internet for outside business interests.

# Email Policy

## Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it’s important for users to understand the appropriate use of electronic communications.

## Purpose

The purpose of this email policy is to ensure the proper use of PXL email system and make users aware of what PXL deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within PXL Network.

## Scope

This policy covers appropriate use of any email sent from a PXL email address and applies to all employees, vendors, and agents operating on behalf of PXL.

## Policy

• All use of email must be consistent with PXL policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.  
• PXL email account should be used primarily for PXL business-related purposes; personal communication is permitted on a limited basis, but non-PXL related commercial uses are prohibited.  
• All PXL data contained within an email message or an attachment must be secured according to the Data Protection Standard.  
• Email should be retained only if it qualifies as a PXL business record. Email is a PXL business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

# Password Construction Guidelines

## Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the Cisco network. This guideline provides best practices for creating secure passwords.

## Purpose

The purpose of this guidelines is to provide best practices for the created of strong passwords

## Scope

This guideline applies to employees, contractors, consultants, temporary and other workers at Cisco, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

## Policy

All passwords should meet or exceed the following guidelines

Strong passwords have the following characteristics:   
• Contain at least 12 alphanumeric characters.   
• Contain both upper and lower case letters.   
• Contain at least one number (for example, 0-9).   
• Contain at least one special character (for example,!$%^&\*()\_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:   
• Contain less than eight characters.   
• Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.