Types of Security Policies

Promiscuous Policy	No restrictions on usage of system resources
Permissive Policy	Policy begins wide open and only known dangerous services, attacks, and behaviors are blocked Policy should be updated regularly to be effective
Prudent Policy	It provides maximum security while allowing known but necessary dangers It blocks all services and only safe or necessary services are individually enabled; everything is logged
Paranoid Policy	It forbids everything. There is either severely limited Internet usage or no Internet connection

Examples of Security Policies

Access-control Policy
Defines the resources being protected and the rules that control access to them

User-account Policy
Defines the user account creation process, account authority, and rights and responsibilities

Remote-access Policy
Defines who can have remote access, and the access medium and remote access security controls

Information-protection Policy
Defines the sensitivity levels of information, who may have access, how it is stored and transmitted, and how it should be deleted from storage media

Firewall-management Policy
Defines access, management, and monitoring of the organization's firewalls

Special-access Policy
Defines the terms and conditions for granting special access to system resources

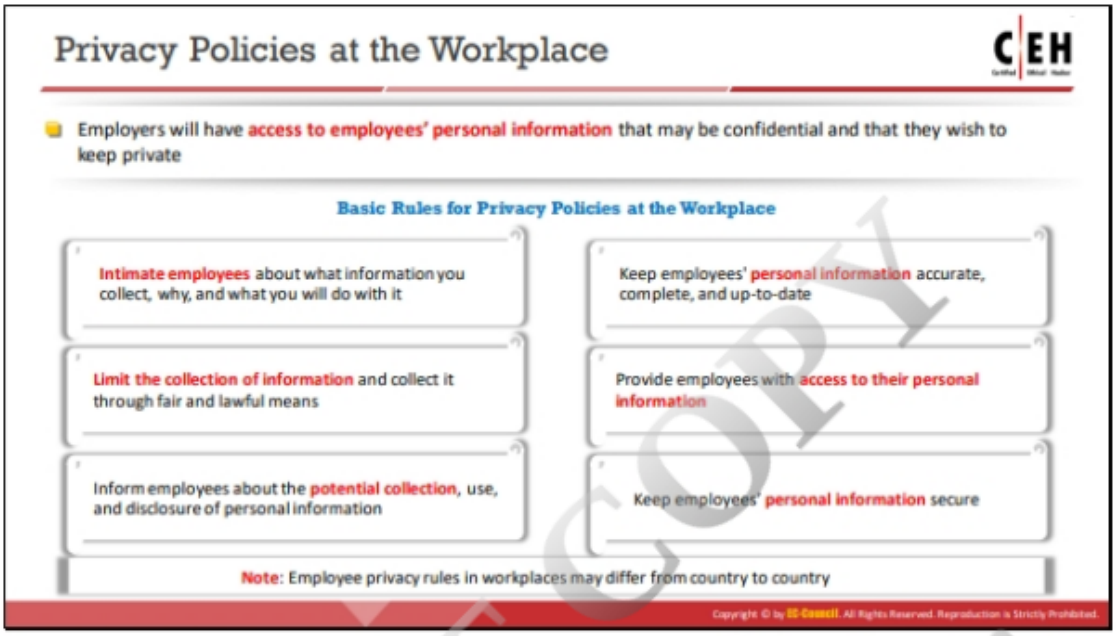
Network-connection Policy
Defines who can install new resources on the network, approve the installation of new devices, document network changes, and other tasks

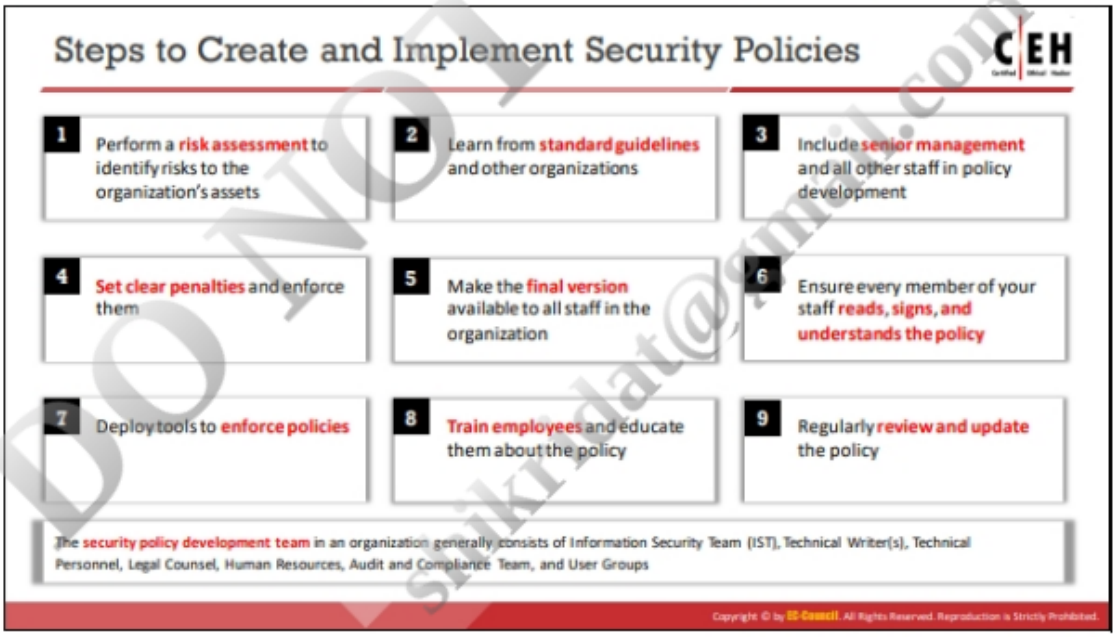
Email-security Policy
Created to govern the proper usage of corporate email

Passwords Policy
Provides guidelines for using strong password protection for the organization's resources

Acceptable-use Policy
Defines the acceptable use of system resources

Notes:





Notes: _____