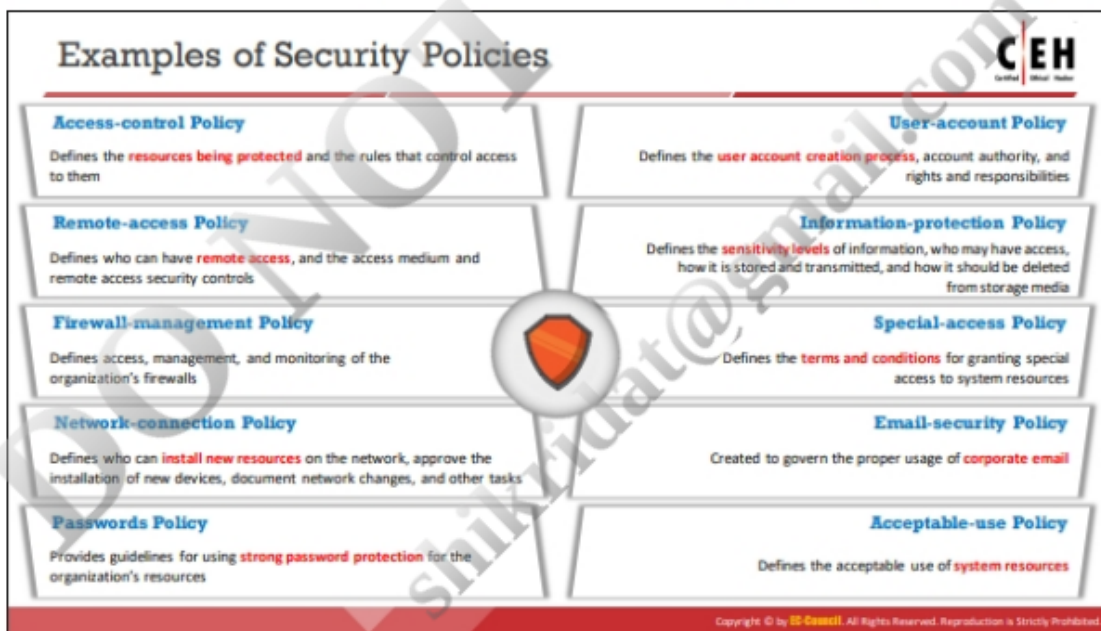


Types of Security Policies		CEH
Promiscuous Policy	<ul style="list-style-type: none"> <li>No restrictions on usage of system resources</li> </ul>	
Permissive Policy	<ul style="list-style-type: none"> <li>Policy begins wide open and only known dangerous services, attacks, and behaviors are blocked</li> <li>Policy should be updated regularly to be effective</li> </ul>	
Prudent Policy	<ul style="list-style-type: none"> <li>It provides maximum security while allowing known but necessary dangers</li> <li>It blocks all services and only safe or necessary services are individually enabled; everything is logged</li> </ul>	
Paranoid Policy	<ul style="list-style-type: none"> <li>It forbids everything. There is either severely limited Internet usage or no Internet connection</li> </ul>	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Notes: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

## Privacy Policies at the Workplace



- Employers will have **access to employees' personal information** that may be confidential and that they wish to keep private

### Basic Rules for Privacy Policies at the Workplace

**Intimate employees** about what information you collect, why, and what you will do with it

Keep employees' **personal information** accurate, complete, and up-to-date

**Limit the collection of information** and collect it through fair and lawful means

Provide employees with **access to their personal information**

Inform employees about the **potential collection**, use, and disclosure of personal information

Keep employees' **personal information** secure

**Note:** Employee privacy rules in workplaces may differ from country to country

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Steps to Create and Implement Security Policies



**1** Perform a **risk assessment** to identify risks to the organization's assets

**2** Learn from **standard guidelines** and other organizations

**3** Include **senior management** and all other staff in policy development

**4** **Set clear penalties** and enforce them

**5** Make the **final version** available to all staff in the organization

**6** Ensure every member of your staff **reads, signs, and understands the policy**

**7** Deploy tools to **enforce policies**

**8** **Train employees** and educate them about the policy

**9** Regularly **review and update** the policy

The **security policy development team** in an organization generally consists of Information Security Team (IST), Technical Writer(s), Technical Personnel, Legal Counsel, Human Resources, Audit and Compliance Team, and User Groups

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

**Notes:**

---

---

---

---

---

---