Cyber Security

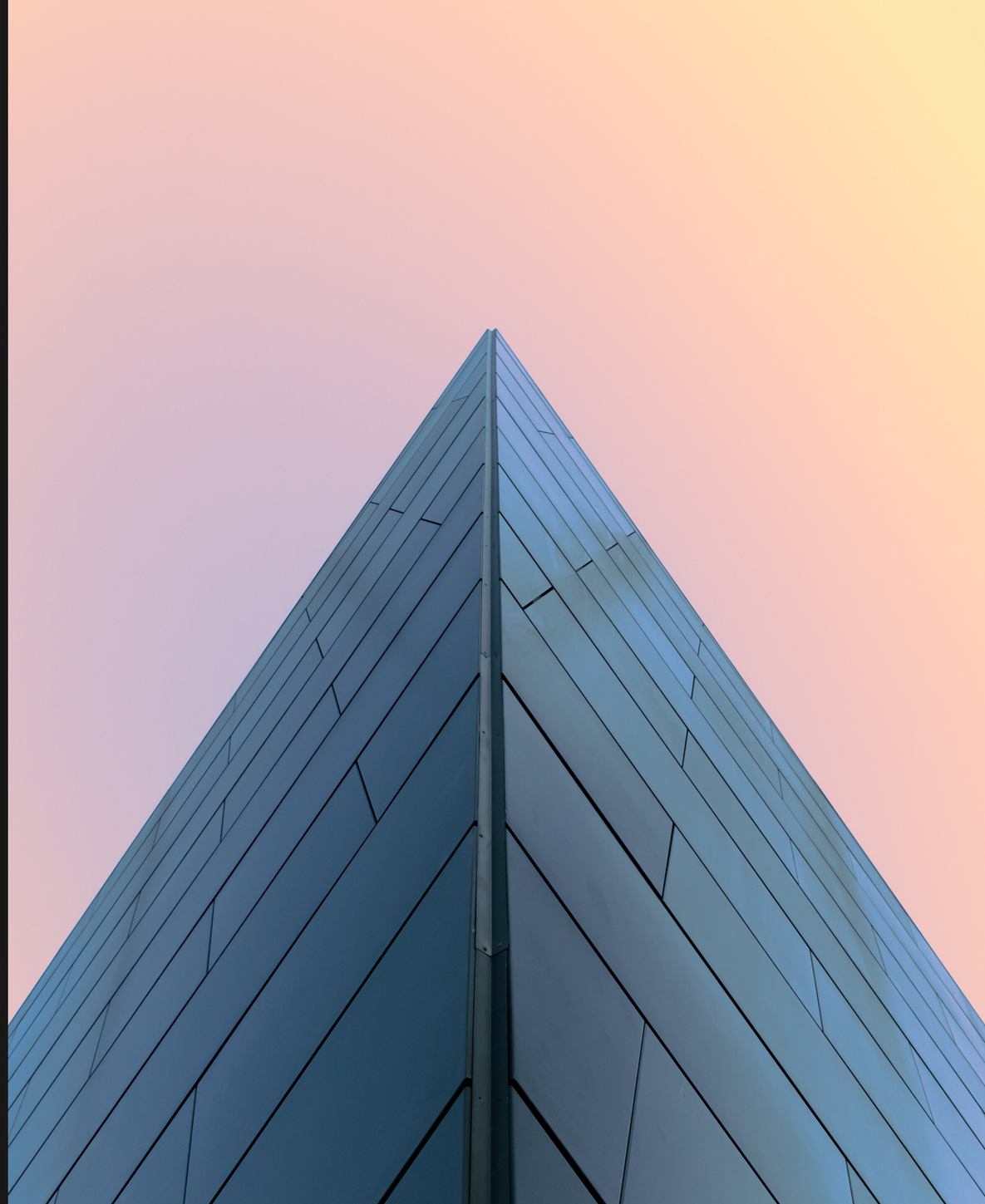
Security Policy

Ali Hamza 021-19-0005
BSCS-VIII

Cybersecurity is an important issue for both IT departments and C-level executives. However, security should be a concern for each employee in an organization, not only IT professionals and top managers.

A cybersecurity policy sets the standards of behavior for activities such as the encryption of email attachments and restrictions on the use of social media.

Cybersecurity policies are important because cyberattacks and data breaches are potentially costly.



Defining a cybersecurity policy

Cybersecurity procedures explain the rules for how employees, consultants, partners, board members, and other end-users access online applications and internet resources, send data over networks, and otherwise practice responsible security.

can be as concise as few pages or dozens of pages based on the organization size and nature

Security policy includes

- Rules for using email encryption
- Steps for accessing work applications remotely
- Guidelines for creating and safeguarding passwords
- Rules on use of social media

Who should write the cybersecurity policies?

- C-level business executives
- The legal department ensures that the policy meets legal requirements and complies with government regulations.
- The human resources (HR) for explaining and enforcing employee policies.
- Procurement personnel may verify that a cloud provider's security meets the organization's cybersecurity policies and verifies the effectiveness of other outsourced relevant services.

Types of Security Policy

Organizational

These policies are a master blueprint of the entire organization's security program.

System-specific

A system-specific policy covers security procedures for an information system or network.

Types of Security Policy

Issue-specific

- rules and regulations for employee use of company assets.
- Access control policies say which employees can access which resources.
- Change management policies provide procedures for changing IT assets so that adverse effects are minimized.
- Disaster recovery policies ensure business continuity after a service disruption. These policies typically are enacted after the damage from an incident has occurred.
- Incident response policies define procedures for responding to a security breach or incident as it is happening.

Thanks