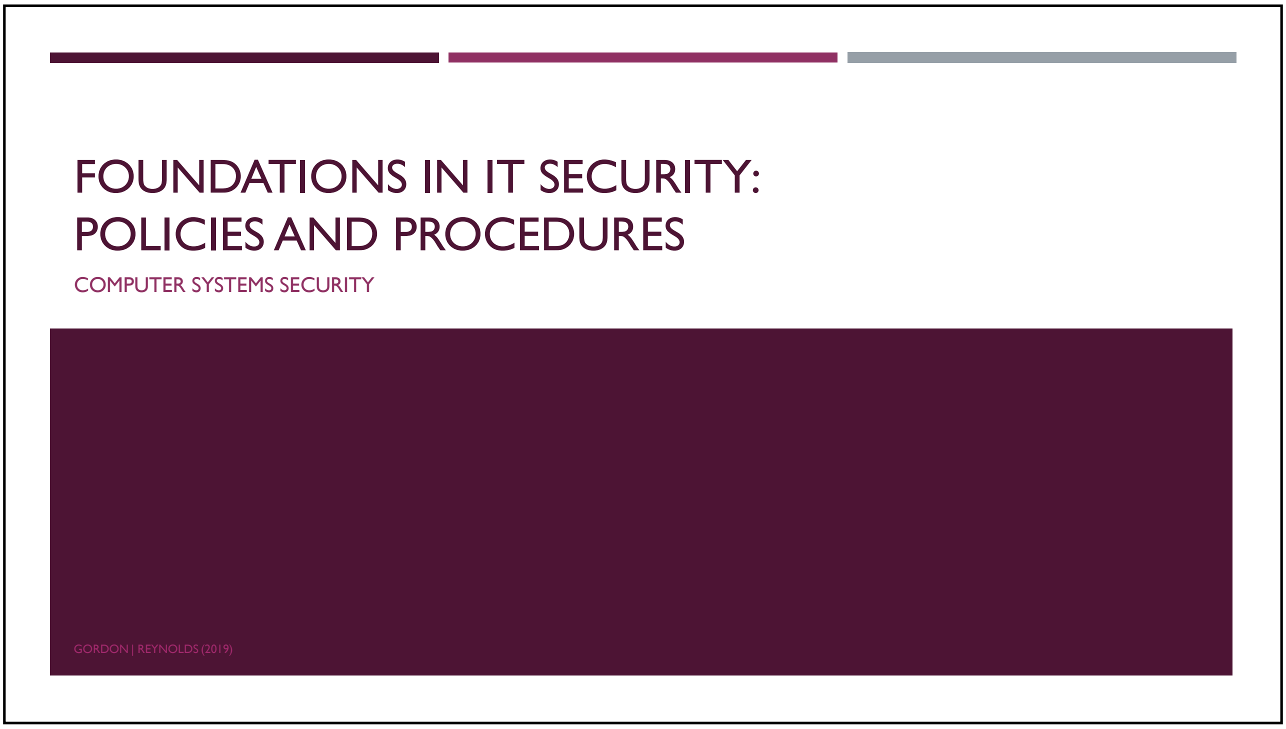
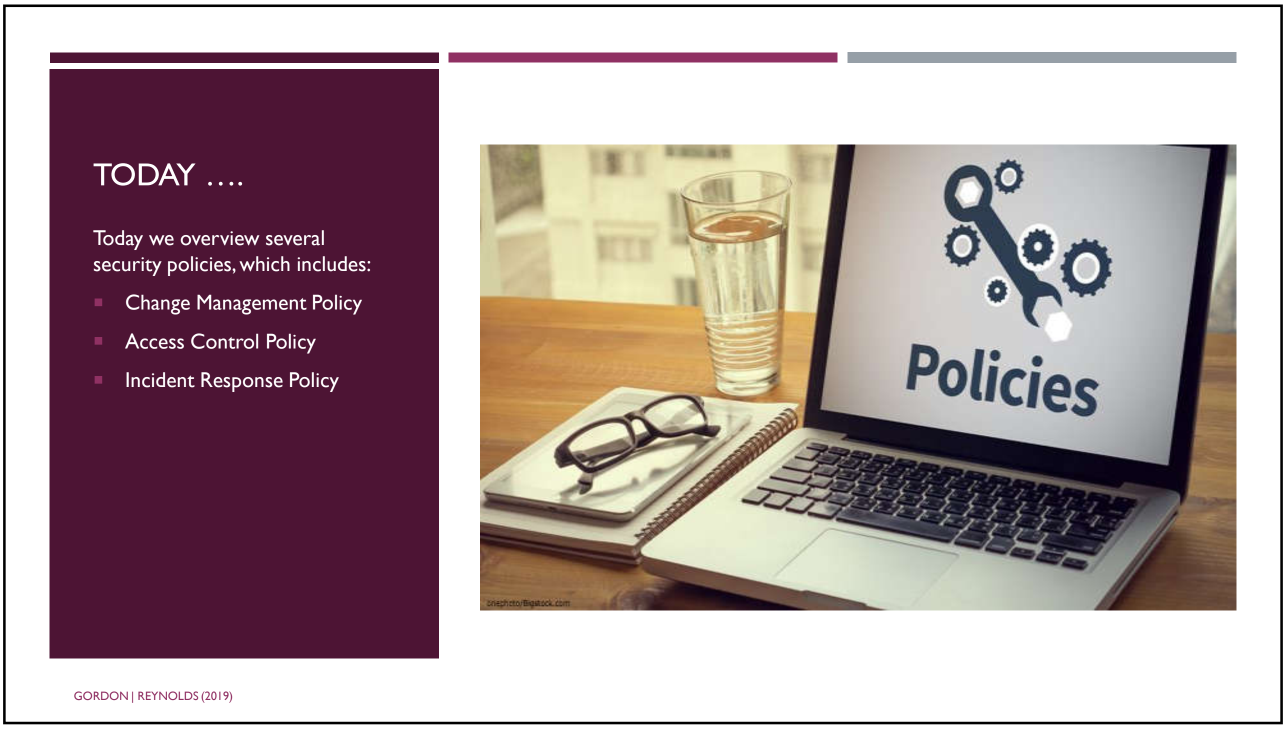


FOUNDATIONS IN IT SECURITY: POLICIES AND PROCEDURES

COMPUTER SYSTEMS SECURITY

GORDON | REYNOLDS (2019)



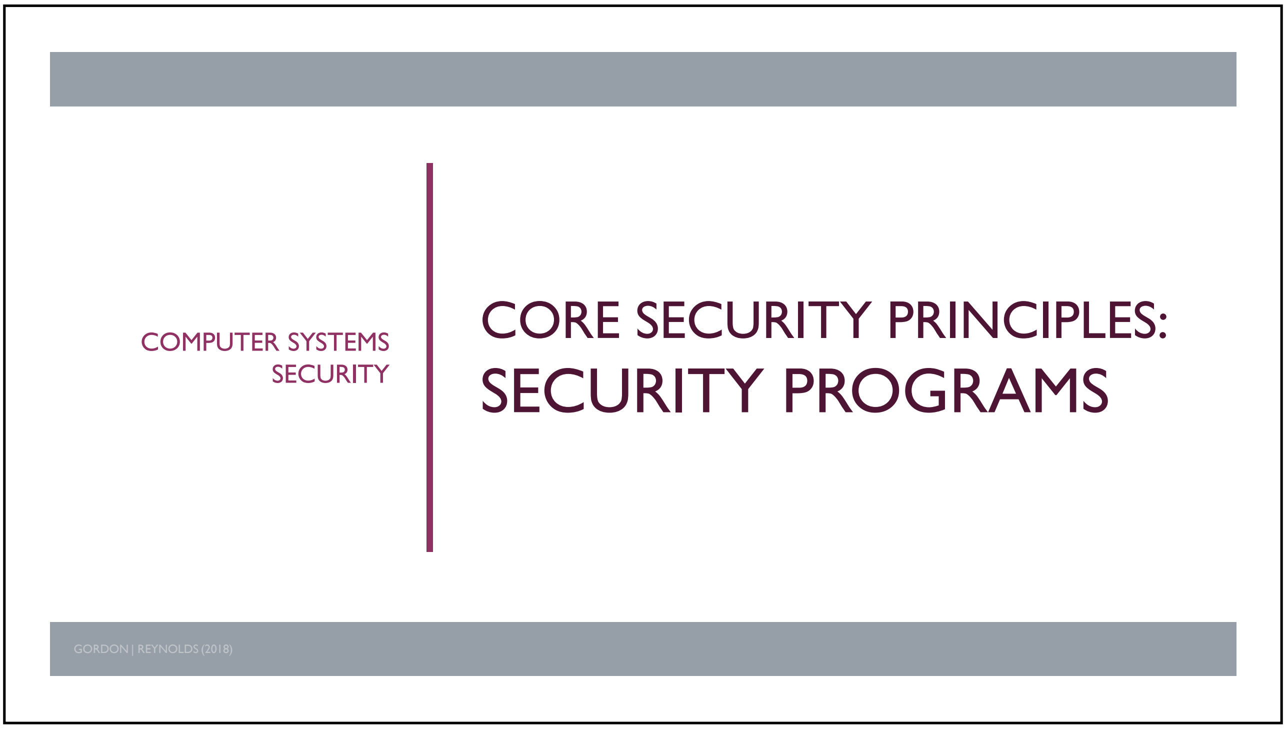
TODAY ….

Today we overview several security policies, which includes:

- Change Management Policy
- Access Control Policy
- Incident Response Policy

onephoto/Bigstock.com

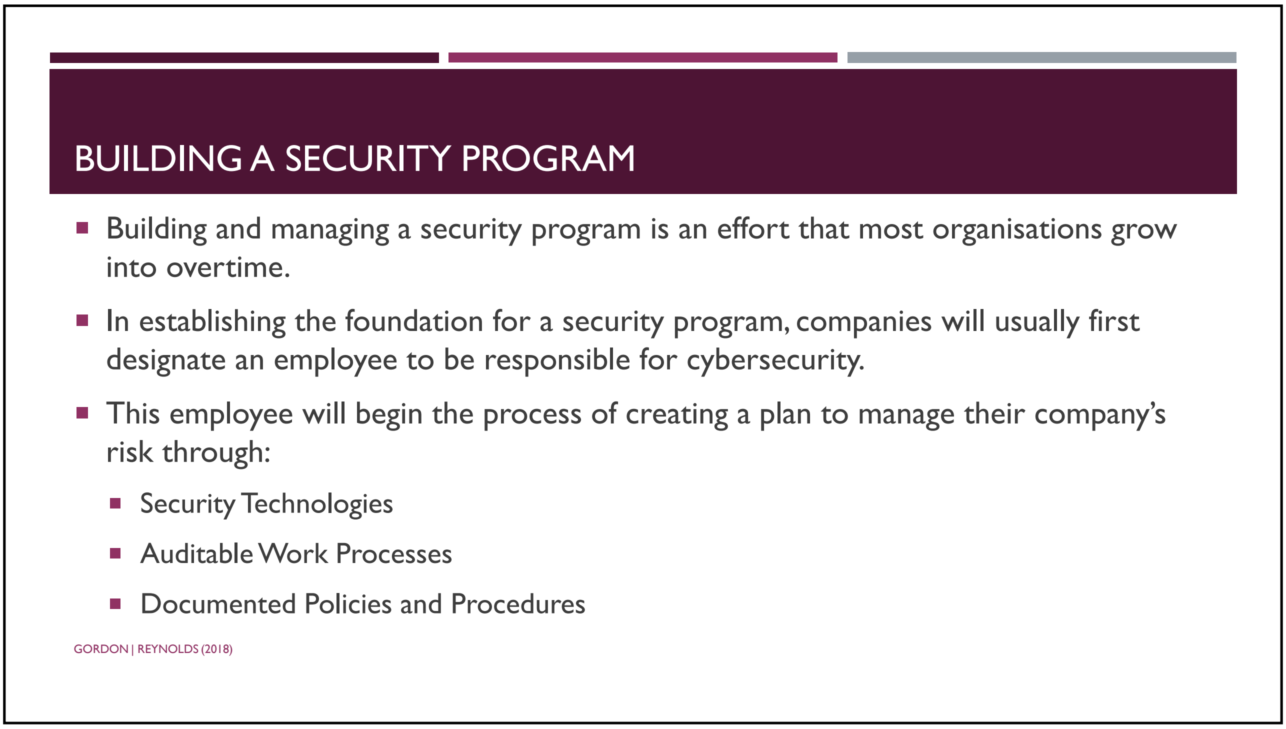
GORDON | REYNOLDS (2019)



COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: SECURITY PROGRAMS

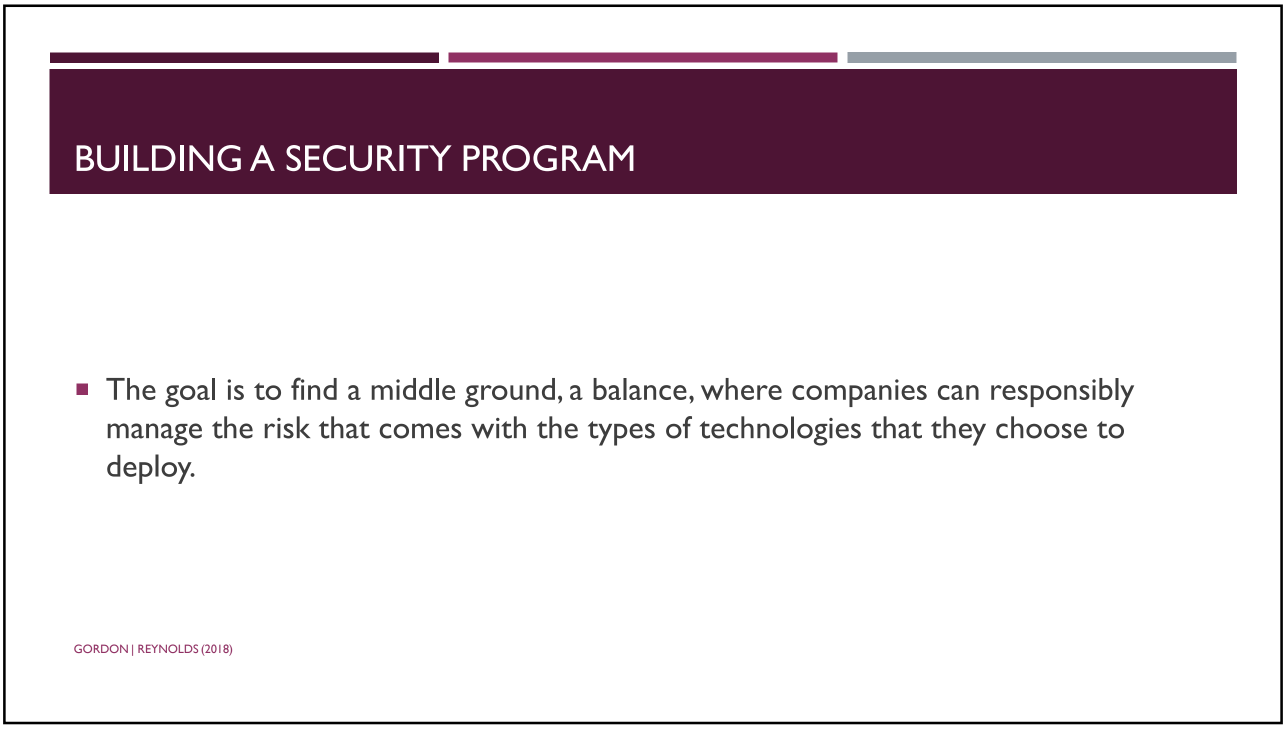
GORDON | REYNOLDS (2018)



BUILDING A SECURITY PROGRAM

- Building and managing a security program is an effort that most organisations grow into overtime.
- In establishing the foundation for a security program, companies will usually first designate an employee to be responsible for cybersecurity.
- This employee will begin the process of creating a plan to manage their company's risk through:
  - Security Technologies
  - Auditable Work Processes
  - Documented Policies and Procedures

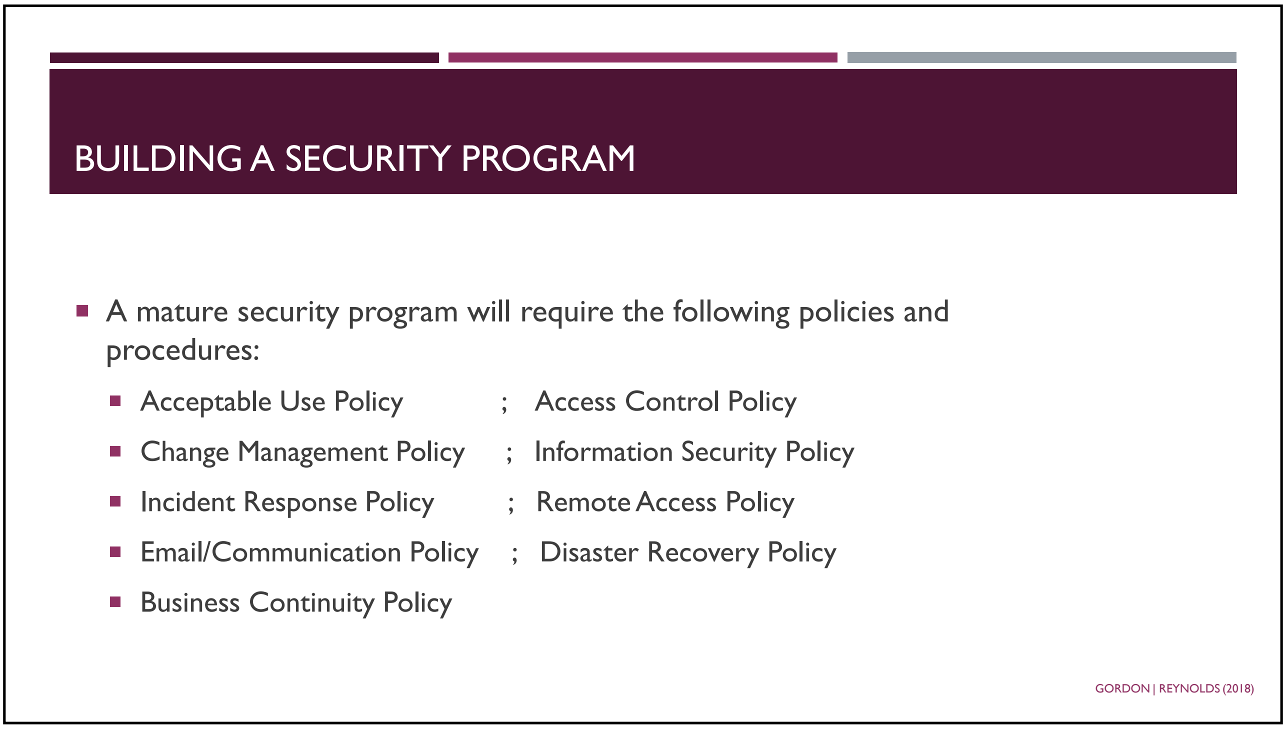
GORDON | REYNOLDS (2018)



BUILDING A SECURITY PROGRAM

- The goal is to find a middle ground, a balance, where companies can responsibly manage the risk that comes with the types of technologies that they choose to deploy.

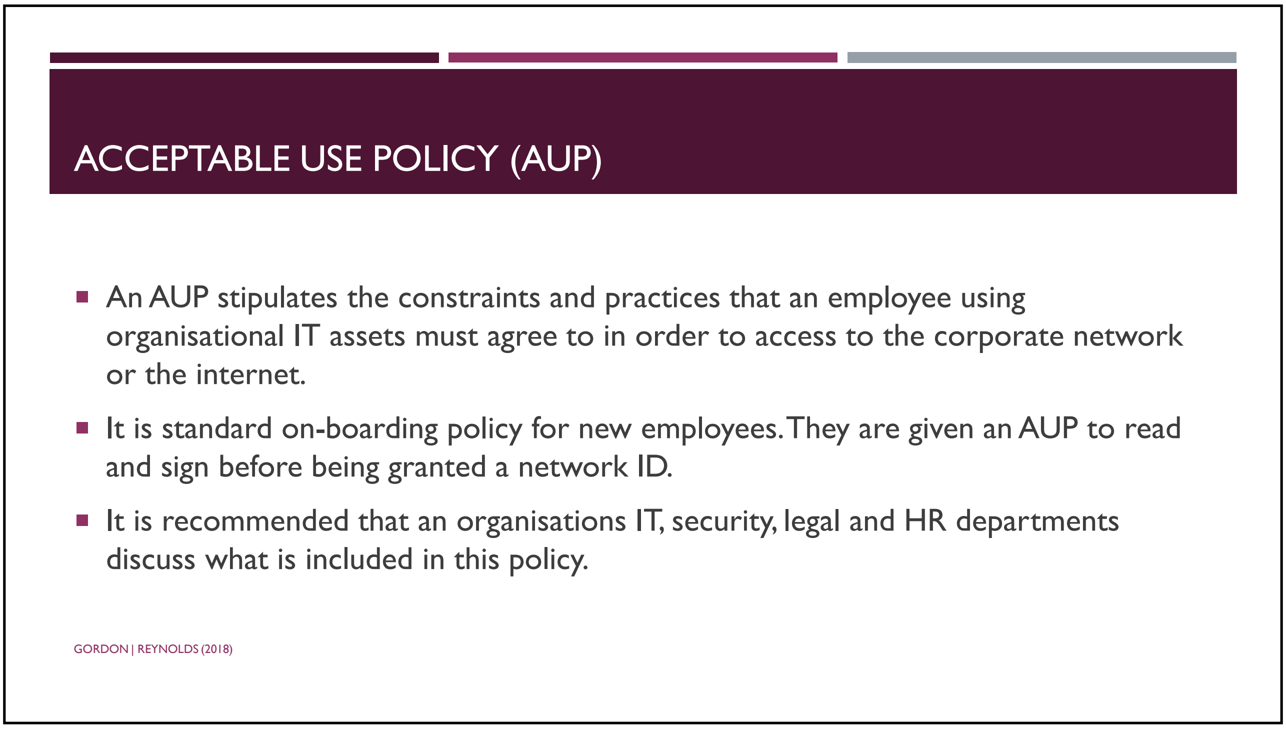
GORDON | REYNOLDS (2018)



BUILDING A SECURITY PROGRAM

- A mature security program will require the following policies and procedures:
  - Acceptable Use Policy ; Access Control Policy
  - Change Management Policy ; Information Security Policy
  - Incident Response Policy ; Remote Access Policy
  - Email/Communication Policy ; Disaster Recovery Policy
  - Business Continuity Policy

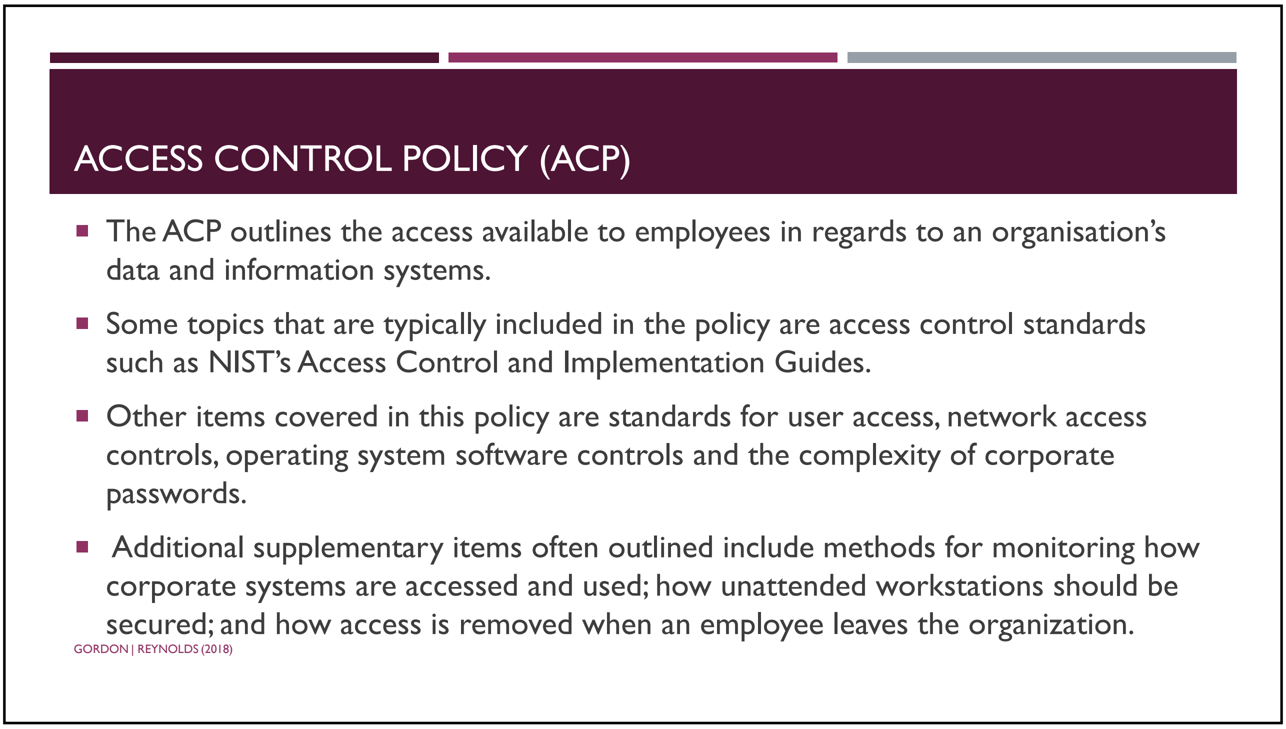
GORDON | REYNOLDS (2018)



ACCEPTABLE USE POLICY (AUP)

- An AUP stipulates the constraints and practices that an employee using organisational IT assets must agree to in order to access to the corporate network or the internet.
- It is standard on-boarding policy for new employees. They are given an AUP to read and sign before being granted a network ID.
- It is recommended that an organisations IT, security, legal and HR departments discuss what is included in this policy.

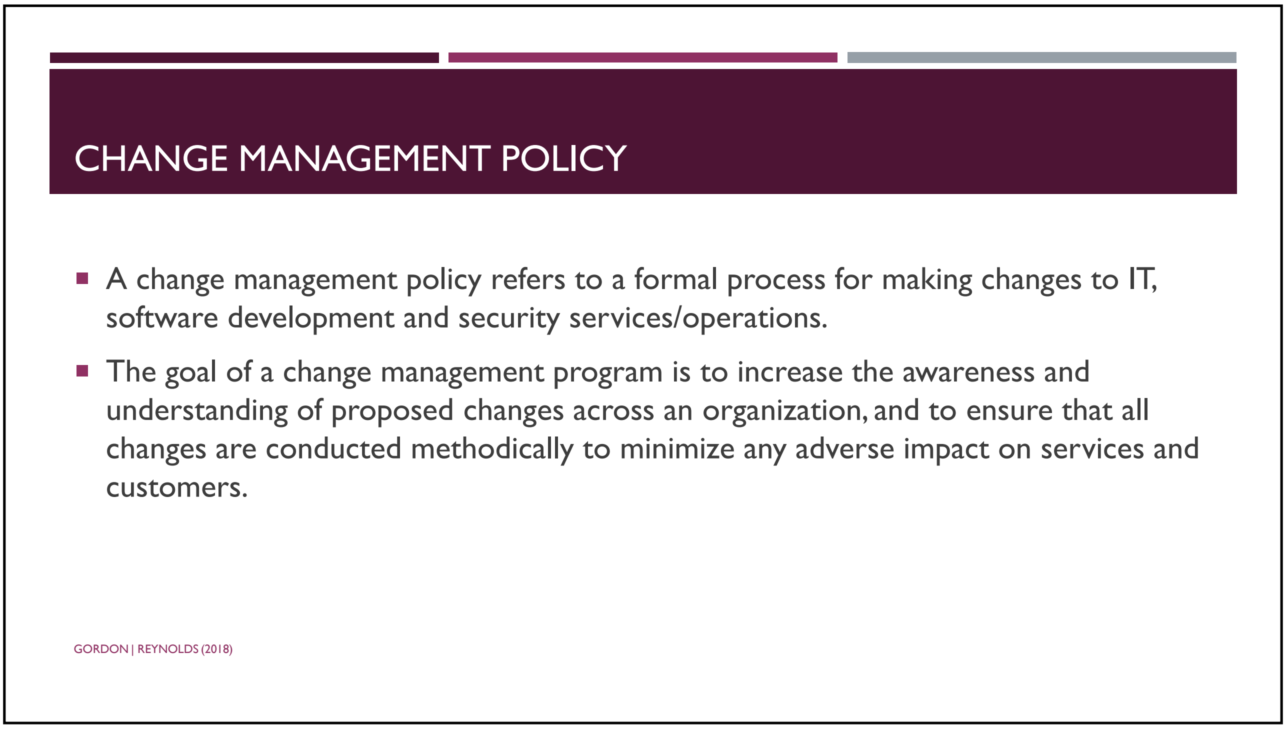
GORDON | REYNOLDS (2018)



ACCESS CONTROL POLICY (ACP)

- The ACP outlines the access available to employees in regards to an organisation's data and information systems.
- Some topics that are typically included in the policy are access control standards such as NIST's Access Control and Implementation Guides.
- Other items covered in this policy are standards for user access, network access controls, operating system software controls and the complexity of corporate passwords.
- Additional supplementary items often outlined include methods for monitoring how corporate systems are accessed and used; how unattended workstations should be secured; and how access is removed when an employee leaves the organization.

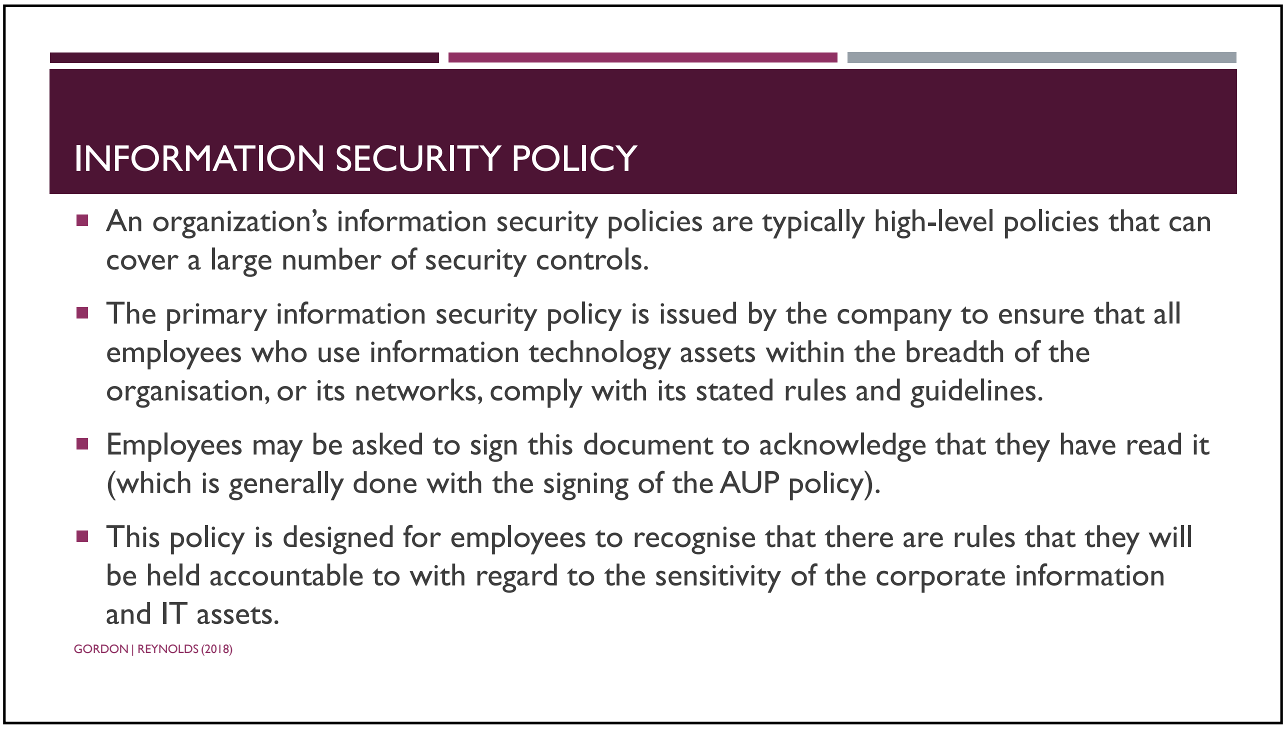
GORDON | REYNOLDS (2018)



CHANGE MANAGEMENT POLICY

- A change management policy refers to a formal process for making changes to IT, software development and security services/operations.
- The goal of a change management program is to increase the awareness and understanding of proposed changes across an organization, and to ensure that all changes are conducted methodically to minimize any adverse impact on services and customers.

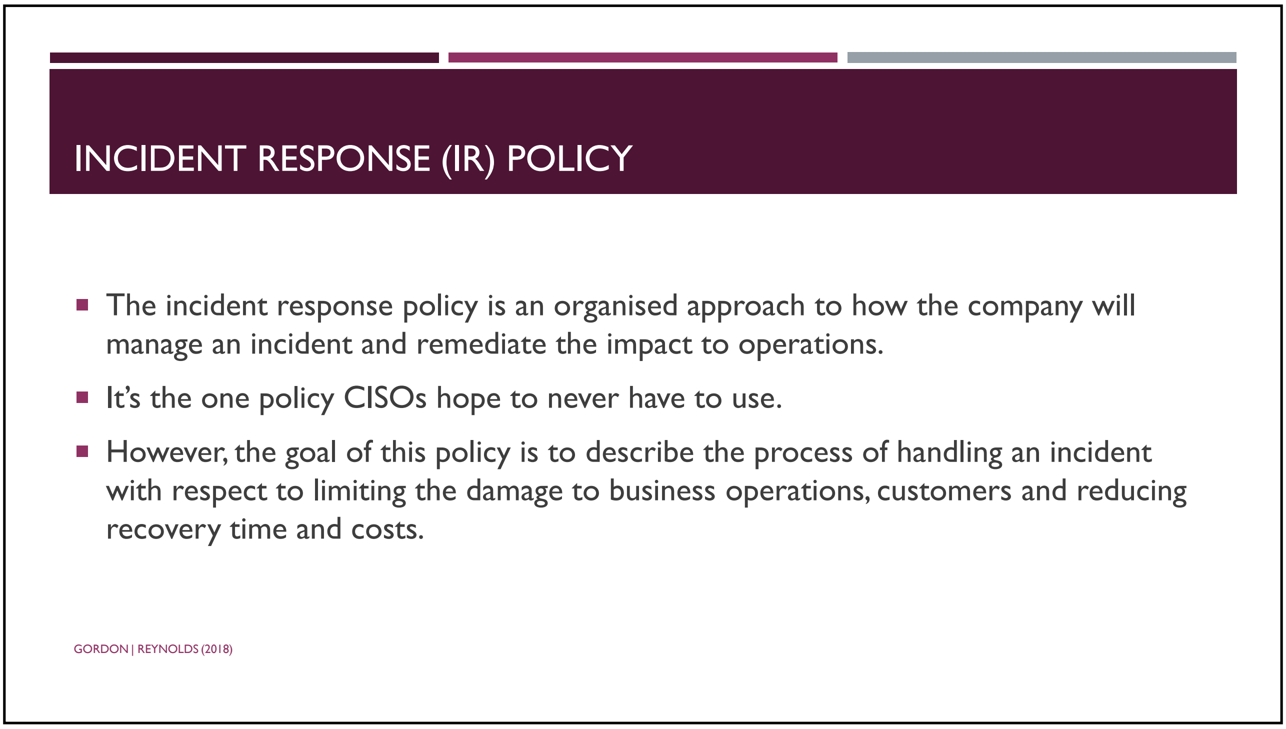
GORDON | REYNOLDS (2018)



INFORMATION SECURITY POLICY

- An organization's information security policies are typically high-level policies that can cover a large number of security controls.
- The primary information security policy is issued by the company to ensure that all employees who use information technology assets within the breadth of the organisation, or its networks, comply with its stated rules and guidelines.
- Employees may be asked to sign this document to acknowledge that they have read it (which is generally done with the signing of the AUP policy).
- This policy is designed for employees to recognise that there are rules that they will be held accountable to with regard to the sensitivity of the corporate information and IT assets.

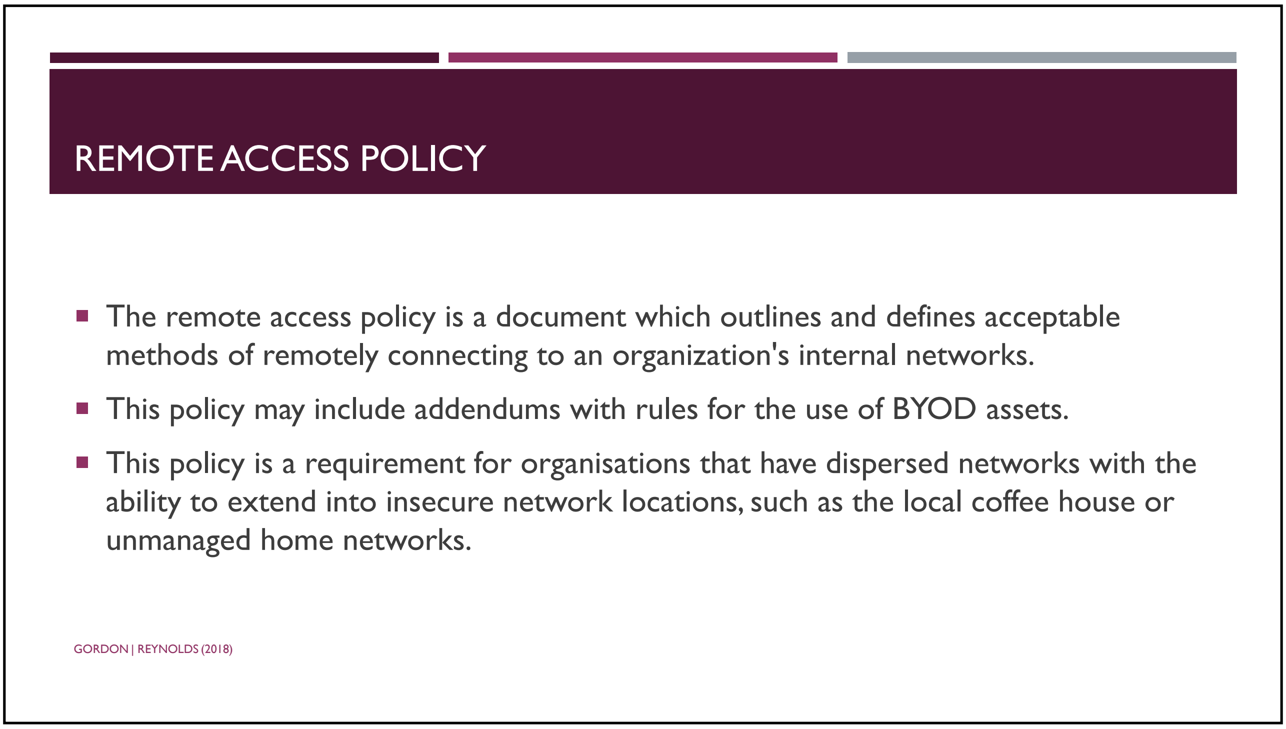
GORDON | REYNOLDS (2018)



INCIDENT RESPONSE (IR) POLICY

- The incident response policy is an organised approach to how the company will manage an incident and remediate the impact to operations.
- It’s the one policy CISOs hope to never have to use.
- However, the goal of this policy is to describe the process of handling an incident with respect to limiting the damage to business operations, customers and reducing recovery time and costs.

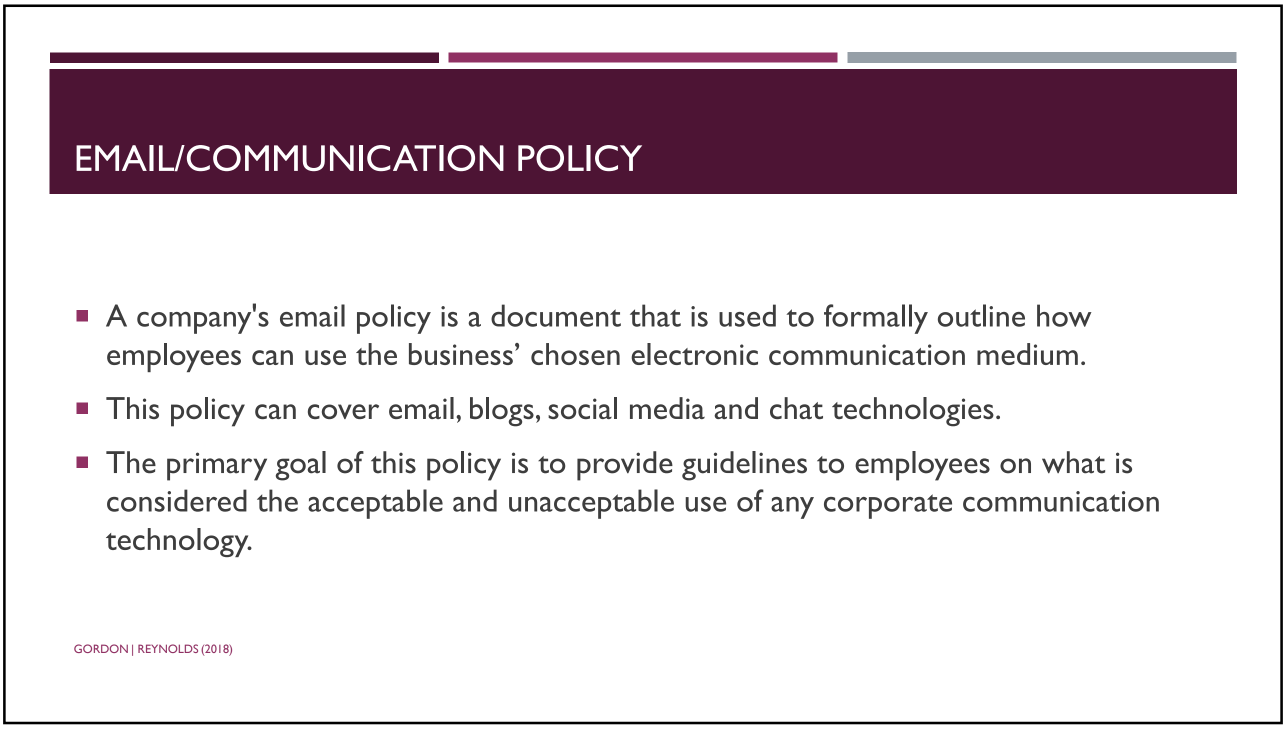
GORDON | REYNOLDS (2018)



REMOTE ACCESS POLICY

- The remote access policy is a document which outlines and defines acceptable methods of remotely connecting to an organization's internal networks.
- This policy may include addendums with rules for the use of BYOD assets.
- This policy is a requirement for organisations that have dispersed networks with the ability to extend into insecure network locations, such as the local coffee house or unmanaged home networks.

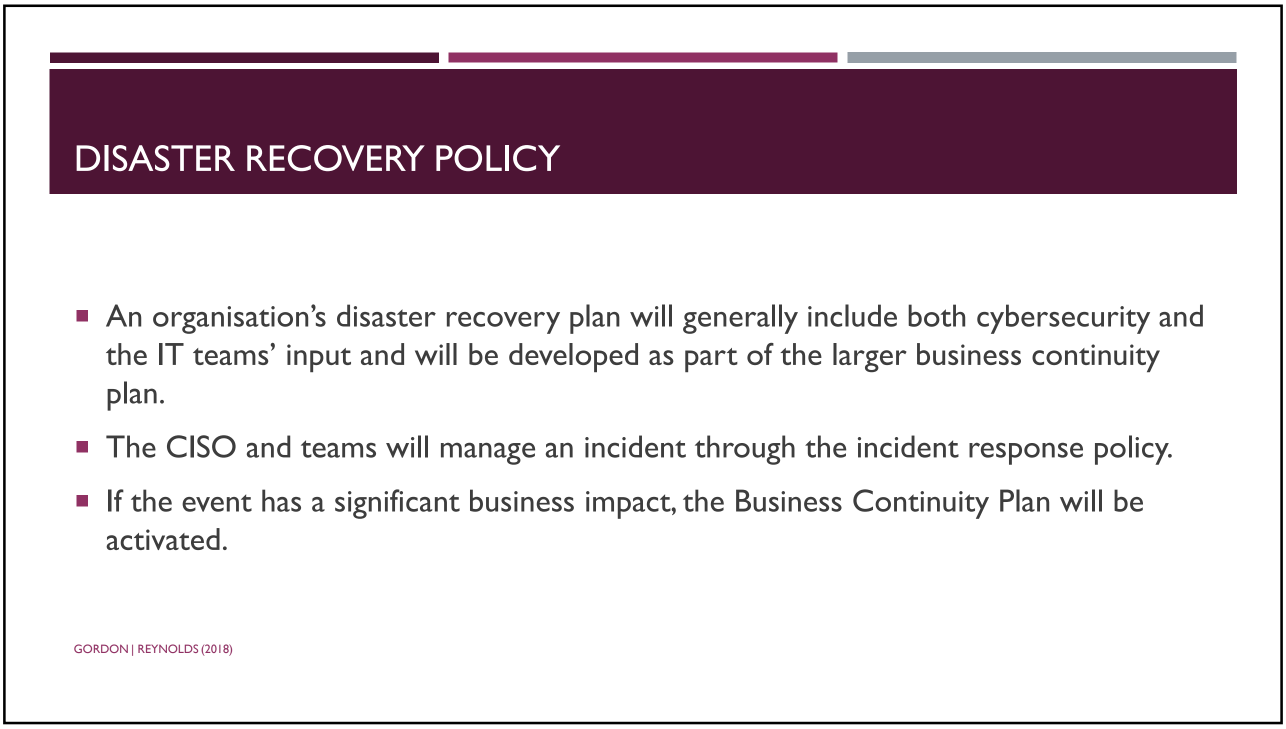
GORDON | REYNOLDS (2018)



EMAIL/COMMUNICATION POLICY

- A company's email policy is a document that is used to formally outline how employees can use the business' chosen electronic communication medium.
- This policy can cover email, blogs, social media and chat technologies.
- The primary goal of this policy is to provide guidelines to employees on what is considered the acceptable and unacceptable use of any corporate communication technology.

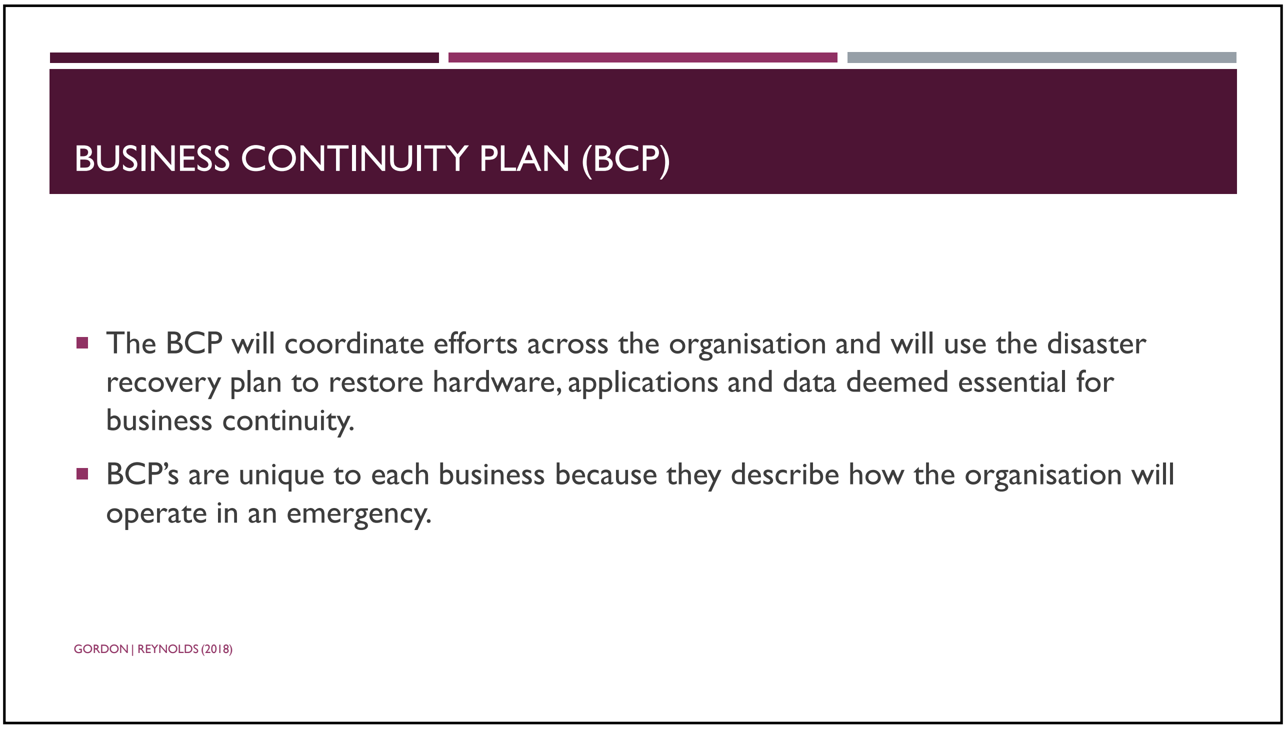
GORDON | REYNOLDS (2018)



DISASTER RECOVERY POLICY

- An organisation's disaster recovery plan will generally include both cybersecurity and the IT teams' input and will be developed as part of the larger business continuity plan.
- The CISO and teams will manage an incident through the incident response policy.
- If the event has a significant business impact, the Business Continuity Plan will be activated.

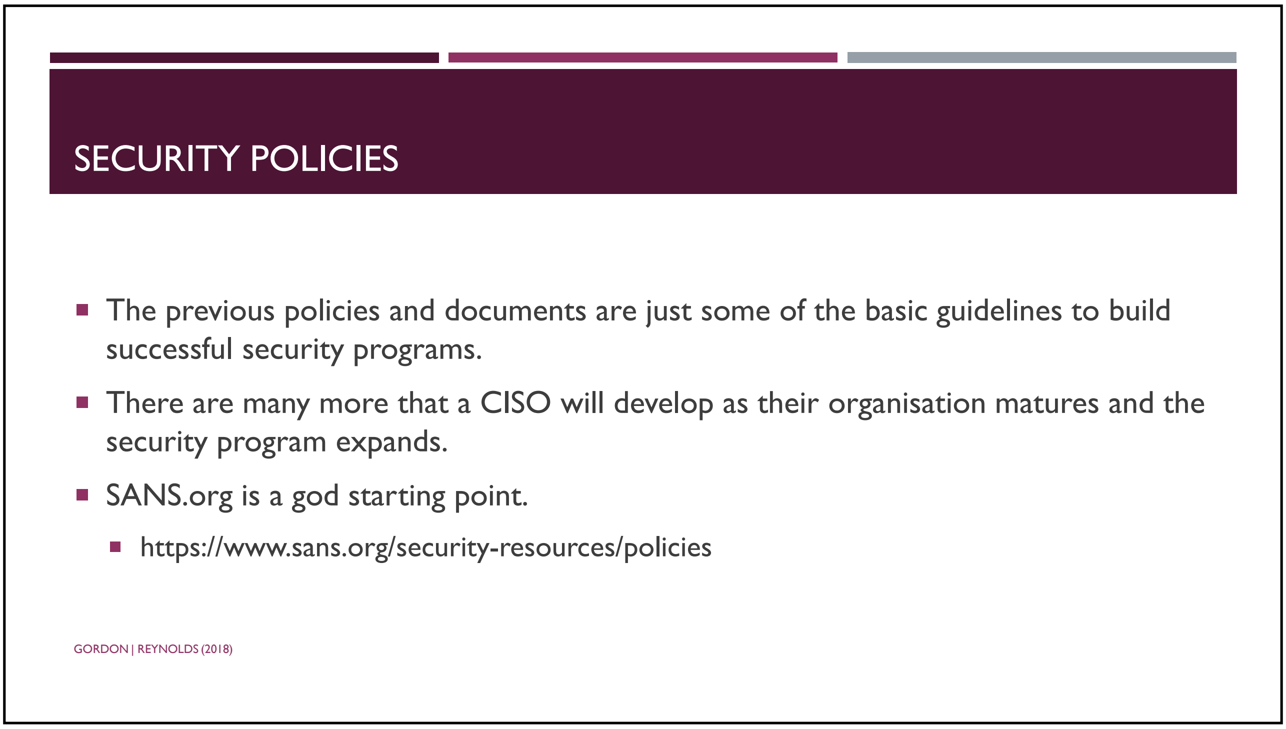
GORDON | REYNOLDS (2018)



BUSINESS CONTINUITY PLAN (BCP)

- The BCP will coordinate efforts across the organisation and will use the disaster recovery plan to restore hardware, applications and data deemed essential for business continuity.
- BCP's are unique to each business because they describe how the organisation will operate in an emergency.

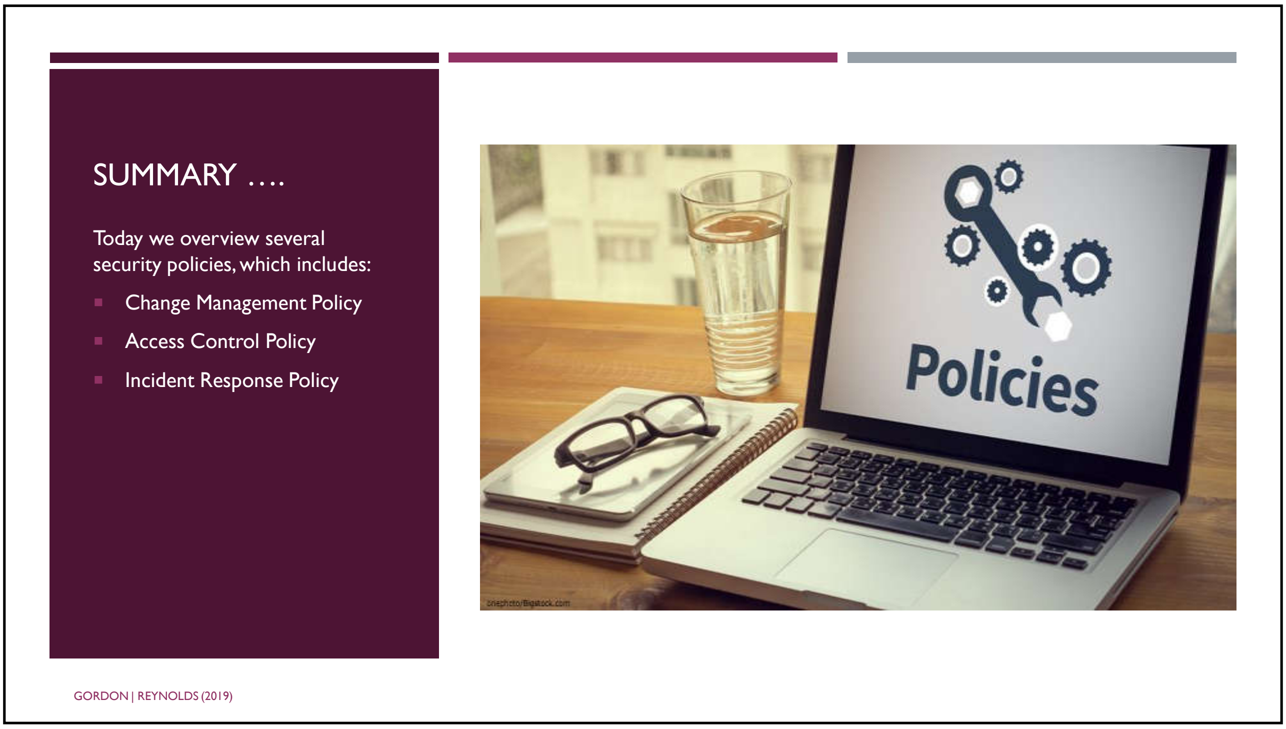
GORDON | REYNOLDS (2018)



SECURITY POLICIES

- The previous policies and documents are just some of the basic guidelines to build successful security programs.
- There are many more that a CISO will develop as their organisation matures and the security program expands.
- SANS.org is a god starting point.
  - https://www.sans.org/security-resources/policies

GORDON | REYNOLDS (2018)



SUMMARY ….

Today we overview several security policies, which includes:

- Change Management Policy
- Access Control Policy
- Incident Response Policy

GORDON | REYNOLDS (2019)