CLEAR LOOP SECURITY

PREPARE/PROTECT/RECOVER

The ~~House~~ ISMS that ~~Jackie~~ You Built – Worksheet

For the Leeds Cyber Security Conference 2025

“Company Company” also known as: _____

Produces/sells/provides: _____

Clients/service users: _____

Unique selling point: _____

CLEAR LOOP SECURITY
PREPARE/PROTECT/RECOVER

4.1 Context

External factors – PESTLE analysis

Factor	Explanation	Issues	Who Cares About This?
Political	How the government intervenes in the economy; for example, employment law, health, education, and national infrastructure		
Economic	Interest rates, exchange rates, and other factors that affect operations and decision-making		
Social	Cultural aspects and health consciousness, population growth rate, age distribution, career attitudes, particularly to the degree that these may inform how an organisation operates		
Technological	Automation, technology penetration and the rate of technological change, which may determine costs, quality, outsourcing, and lead to innovation		
Legal	The legal environment in which an organisation operates		
Environmental	Ecological and environmental aspects such as weather and climate change; growing awareness of the potential impacts of climate change may affect products offered		

4.1 Context

Internal factors – 7S analysis

Factor	Explanation	Issues	Who Cares About This?
Strategy	Purpose of the organisation and the way they seek to enhance its competitive advantage		
Structure	Division of activities; integration and coordination mechanisms		
Systems	Formal procedures for measurement, reward and resource allocation		
Shared Values	The core values of the organisation that guide employee behaviour and organisational actions		
Skills	The organisation's core competencies and distinctive capabilities		
Staff	The organisation's human resources, demographic, educational and attitudinal characteristics		
Style	Typical behaviour patterns of key groups, such as managers, and other professionals		

CLEAR LOOP SECURITY
PREPARE/PROTECT/RECOVER

4.2 Interested Parties

Party	Requirements	How Addressed

CLEAR LOOP SECURITY
PREPARE/PROTECT/RECOVER

Threat Tree

Top-Level Source	Actor/Source	Motive	Outcome
Human - technical	Insider	Accidental	Disclosure
Human - technical	Insider	Accidental	Modification
Human - technical	Insider	Accidental	Interruption
Human - technical	Insider	Accidental	Destruction/Loss
Human - technical	Insider	Deliberate	Disclosure
Human - technical	Insider	Deliberate	Modification
Human - technical	Insider	Deliberate	Interruption
Human - technical	Insider	Deliberate	Destruction/Loss
Human - technical	External attacker	Accidental	Disclosure
Human - technical	External attacker	Accidental	Modification
Human - technical	External attacker	Accidental	Interruption
Human - technical	External attacker	Accidental	Destruction/Loss
Human - technical	External attacker	Deliberate	Disclosure
Human - technical	External attacker	Deliberate	Modification
Human - technical	External attacker	Deliberate	Interruption
Human - technical	External attacker	Deliberate	Destruction/Loss
Human - physical	Insider	Accidental	Disclosure
Human - physical	Insider	Accidental	Modification
Human - physical	Insider	Accidental	Interruption
Human - physical	Insider	Accidental	Destruction/Loss
Human - physical	Insider	Deliberate	Disclosure
Human - physical	Insider	Deliberate	Modification
Human - physical	Insider	Deliberate	Interruption
Human - physical	Insider	Deliberate	Destruction/Loss
Human - physical	External attacker	Accidental	Disclosure
Human - physical	External attacker	Accidental	Modification
Human - physical	External attacker	Accidental	Interruption
Human - physical	External attacker	Accidental	Destruction/Loss
Human - physical	External attacker	Deliberate	Disclosure
Human - physical	External attacker	Deliberate	Modification
Human - physical	External attacker	Deliberate	Interruption
Human - physical	External attacker	Deliberate	Destruction/Loss
Other sources	Software/hardware defects	n/a	Disclosure
Other sources	Software/hardware defects	n/a	Modification
Other sources	Software/hardware defects	n/a	Interruption
Other sources	Software/hardware defects	n/a	Destruction/Loss
Other sources	System crashes	n/a	Disclosure
Other sources	System crashes	n/a	Modification
Other sources	System crashes	n/a	Interruption
Other sources	System crashes	n/a	Destruction/Loss
Other sources	Malicious code	n/a	Disclosure
Other sources	Malicious code	n/a	Modification

- **Organisational Controls**
- Policies for information security
- Information security roles and responsibilities
- Segregation of duties
- Management responsibilities
- Contact with authorities
- Contact with special interest groups
- Threat intelligence
- Information security in project management
- Inventory of information and other associated assets
- Acceptable use of information and other associated assets
- Return of assets
- Classification of information
- Labelling of information
- Information transfer
- Access control
- Identity management
- Authentication information
- Access rights
- Information security in supplier relationships
- Addressing information security within supplier agreements
- Managing information security in the information and communication technology (ICT) supply chain
- Monitoring, review and change management of supplier services
- Information security for use of cloud services
- Information security incident management planning and preparation
- Assessment and decision on information security events
- Response to information security incidents
- Learning from information security incidents
- Collection of evidence
- Information security during disruption
- ICT readiness for business continuity
- Legal, statutory, regulatory and contractual requirements
- Intellectual property rights
- Protection of records
- Privacy and protection of personal identifiable information (PII)
- Independent review of information security
- Compliance with policies, rules and standards for information security
- Documented operating procedures
- **People Controls**
- Screening
- Terms and conditions of employment
- Information security awareness, education and training
- Disciplinary process
- Responsibilities after termination or change of employment
- Confidentiality or non-disclosure agreements
- Remote working
- Information security event reporting
- **Physical Controls**
- Physical security perimeters
- Physical entry
- Securing offices, rooms and facilities
- Physical security monitoring
- Protecting against physical and environmental threats
- Working in secure areas
- Clear desk and clear screen
- Equipment siting and protection
- Security of assets off-premises
- Storage media
- Supporting utilities
- Cabling security
- Equipment maintenance
- Secure disposal or re-use of equipment
- **Technological Controls**
- User end point devices
- Privileged access rights
- Information access restriction
- Access to source code
- Secure authentication
- Capacity management
- Protection against malware
- Management of technical vulnerabilities
- Configuration management
- Information deletion
- Data masking
- Data leakage prevention
- Information backup
- Redundancy of information processing facilities
- Logging
- Monitoring activities
- Clock synchronization
- Use of privileged utility programs
- Installation of software on operational systems
- Networks security
- Security of network services
- Segregation of networks
- Web filtering
- Use of cryptography
- Secure development life cycle
- Application security requirements
- Secure system architecture and engineering principles
- Secure coding
- Security testing in development and acceptance
- Outsourced development
- Separation of development, test and production environments
- Change management
- Test information
- Protection during audit