**Example security plan**

[Name of organisation and author's name] Security Plan

**i. Executive summary**

Objective: Briefly describe the purpose and goals of the security plan. For example:

*This security plan's objectives are to review current and future:*

* *Threats*
* *Vulnerabilities*
* *Security measures*

*at site [x], following a security brach on [y] date.*

**ii. Introduction**

Scope: Define the security plan's scope and limits. For example:

*This security plan reviews physical security measures at [X]'s headquarters. It does not include any satellite office or location.*

Key stakeholders: Identify the individuals or groups responsible for security.

Legal and regulatory compliance: List relevant laws, regulations and standards that must be followed.

**iii. Threat assessment**

Identify, describe and list potential threats. These can include:

**Natural disasters**

* Flood
* Heatwave
* Landslide

**Cyber attacks**

* Denial of service
* Ransomware

**Physical failures**

* Breaches
* Unauthorised visitors
* Theft

**Terrorist threat**

Martyn's Law will likely focus a threat assessment on terrorist attacks. Therefore, it may include the following attack methods:

* Firearms attacks
* Bladed weapon attack
* Vehicle as weapon attack
* Explosives – carried or concealed
* Explosives – person borne
* Explosives – vehicle (also drone) borne
* Drone as a weapon
* Drone borne agents – CBRN
* Chemical agent attack
* Biological agent attack
* Radiological agent attack

An example of factors that may increase the likelihood of a terrorist attack include:

* Site importance
* Very important people
* Current security measures
* Accessibility
* Adjacent public places
* Public transport
* Structural resilience
* Other buildings/structures in proximity
* Internal security measures
* Insider threat and internal controls

**Risk Analysis**

Assess the likelihood and impact of each threat to the organisation. A common method for a risk analysis is to multiple the likelihood of an event by its impact on the business. For example:

The likelihood of an acid attack is 3 out of 5 and the impact on the business of an acid attack is 4 out of 5. Therefore, the risk is 3 x 4 = 12 out of a possible 25 (5 x 5). We could then visualise the risk on a matrix as we can with [SIRV](https://getsirv.com/):

In addition, we can capture this information and have a 'live' risk analysis that changes over time.

**Vulnerability Assessment**

Identify current vulnerabilities and weaknesses that could be exploited.

**iv. Security policies and procedures**

**Access Control**

Define types of access and list who has access to what. In addition, include how to gain and revoke access.

**Physical Security**

Describe measures to secure physical locations.

**Information Security**

Explain how sensitive data is protected. For example:

* Encryption
* Password policies
* Data backups
* Data protection impact assessment (DPIA)

**Cybersecurity**

Detail measures to safeguard against cyber threats. For example:

* Firewalls
* Antivirus
* Incident response plans

**Emergency response**

Outline protocols for responding to different types of emergencies (e.g., fire, medical, security breach).

**Incident reports**

Describe the [incident report](https://getsirv.com/incident-report/) system.

**Security awareness training**

Explain how employees or relevant individuals receive education about security risks and protocols.

**Security tests and audits**

Describe how regular tests and audits of security measures are conducted.

**v. Physical security**

**Facility security**

Detail the control of physical access to facilities. For example:

* Gates
* Locks
* Alarms
* Fences
* CCTV cameras
* Anti-drone measures
* Access control system
* Security guards

**Visitor control**

Explain the control and management of visitors.

**Asset protection**

Describe the protection for high value assets such as, equipment.

**Security cameras and surveillance**

Discuss the use of security cameras and their monitoring.

**vi. Information security**

* Data classification: Define categories of data and their security requirements.
* Data encryption: Specify encryption methods for sensitive data.
* User authentication: Describe user authentication processes and password policies.
* Data backup and recovery: Detail data backup strategies and disaster recovery plans.
* Security awareness training: Explain how employees or relevant individuals are educated about information security.
* Incident response: Outline the steps to take in the event of a data breach or security incident.

**vii. Cybersecurity**

Firewalls and intrusion detection / prevention: Describe the use of firewalls and intrusion detection/prevention systems.

Antivirus and Malware protection: Explain the use of antivirus software and malware protection.

Patch management: Detail how software updates and patches are managed.

Network security: describe measures to secure networks and communication channels.

Security monitoring and incident response: Explain how cybersecurity incidents are detected and responded to.

**viii. Training and awareness**

Describe the training programs for employees or relevant individuals along with efforts to raise security awareness and promote best practices.

**Martyn's Law: Terrorism protection training**

Under Martyn's Law there's likely to be a focus on:

* Terrorism awareness
* Suspicious activity recognition
* Emergency response procedure
* First Aid and trauma response
* Communication protocols
* Use of security equipment
* De-escalation techniques
* Legal and compliance aspects

**Martyn's Law: Public awareness and communication**

Martyn’s Law wants to ensure staff, the public, visitors, and potentially the wider community, are aware of the risks of terrorism and the measures in place to mitigate these risks. As a result, Martyn’s Law is likely to require a three phase approach:

i) Communication before an incident

* Public awareness: For example, signs about safe escape routes.
* Security culture promotion: For example, encourage the public to report suspicious activity ([read about how 2017 Manchester Arena bombing](https://www.bbc.co.uk/news/uk-england-manchester-54056327) attacker was challenged).
* Broadcast information: For example, use various channels like social media, websites and brochures

ii. Communication during an incident

* Clear and timely Information: For example, prompt messages about type of incident with regular updates.
* Use multiple channels such as, social media, text alerts and [public address systems](https://getsirv.com/2022/12/mass-communication-systems-and-martyns-law/)
* Coordination with authorities such as emergency services and local council

iii. Communication after an incident

* Update the public about the situation, areas to avoid and when it is safe to return to normal activities.
* Support and resources available such as counselling or assistance centres.
* Feedback and learning with the public to gather feedback on the effectiveness of the communication and the overall response.

**ix. Tests and evaluation**

Security audits and assessments: Outline plans for regular security audits and assessments.

Incident exercises: Describe exercises to test the effectiveness of incident response plans.

**x. Compliance and reports**

Compliance Requirements: List specific compliance standards and regulations relevant to the business or situation.

Report procedures: Explain how compliance is monitored and reported.

**xi. Budget and resources**

Budget allocation: Give a cost budget to implement and maintain security measures.

Resource allocation: Identify the personnel and resources necessary for security.

**xii. Review and updates**

Present a review schedule for the security plan. Typically, reviews are annual. However, ad hoc reviews are necessary after a [change in the risk environment](https://www.gov.uk/terrorism-national-emergency) or major security incident.

Describe the security plan.

**xiii. Security plan conclusion**

Summarise the security plan's key points and credits others involved in the plan creation.

**xiv. Appendices**

Add documents, forms, or reference materials.