**Security (Advocate: Manish Gadhvi)**

**P1 Identify types of security risks to organisations.**

|  |
| --- |
| <https://github.com/LBruni98/Reboot-Games-Security-Policy/blob/master/README.md#2-risk-assessment>  <https://github.com/LBruni98/Reboot-Games-Security-Policy/blob/master/README.md#3-threats-in-an-organisation> |
| The links above takes the user to the security policy README file. The first link explains the risks that can occur in an organisation and covered are Theft of Hardware, Data loss/theft and social engineering. The second link explains the threats within the organisation, covered in the file is Malware and viruses. The sections describe how they work, what harm they can do and how it can impact a business. |

**P2 Describe organisational security procedures.**

|  |
| --- |
| <https://github.com/LBruni98/Reboot-Games-Security-Policy/blob/master/README.md#5-security-procedures> |
| The link above takes the user to the security policy README file, specifically the section on ‘Security Procedures’. Covered are the procedures for logging in, general awareness and entering the establishment. These guidelines direct the employee to carry out for an improved and safer working conditions, as well as list the procedures for each section to be carried out. |

**P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and third party VPNs.**

|  |
| --- |
| <https://github.com/LBruni98/Reboot-Games-Security-Policy/blob/master/README.md#6-the-impact-of-poor-configuration> |
| The link above takes the user to the Reboot Game’s security policy README file, under “The Impact of Poor Configuration”. The section describes what firewall policies and third-party VPNs and how they work before going into the impacts to IT security that they can cause, should the configuration be improper. For instance, it describes that all sorts of network traffic gets let through if the policy is configured to be strict enough. |

**P4 Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.**

|  |
| --- |
| <https://github.com/LBruni98/Reboot-Games-Security-Policy/blob/master/README.md#7-improving-network-security> |
| The link above directs to the Reboot Games security policy readme, under the section, “Improving Network Security”. The section is divided into three sub-headings; DMZ, Static IP and NAT. This section describes what these features are within networking terms and describes what they do before describing what they can do to add security and how they can improve it in a network. |

**P5 Discuss risk assessment procedures.**

|  |
| --- |
| <https://github.com/LBruni98/Reboot-Games-Security-Policy/blob/master/README.md#22-assessment-procedures> |
| The link above takes the user to the security policy repo, mainly the subheading underneath the risks section. This section discusses the risk assessment procedures and follows off from the risks listed in the first part of the section. What this part of the document goes into is by explaining the risk procedures from the risks listed prior, by detailing what the procedure is and how it can help prevent any threats. For instance, with data loss, this can be prevented if any physical medium, such as a USB, is locked away after use. |

**P6 Explain data protection processes and regulations as applicable to an organisation.**

|  |
| --- |
| <https://github.com/LBruni98/Reboot-Games-Security-Policy/blob/master/README.md#8-data-protection-procedures> |
| This link takes the user to the security policy README, under the ‘Data Protection’ section. The section goes into two details about the procedures. The first part of the data protection procedures talks about the compliance to data protection legislation, where the user must comply with the regulations involved and understand their importance and consequences. The second part details the processes of data protection that the user must follow. Covered is how the employees will be notified on how their data will be used and the restrictions of handling and using any sort of data. |

**P7 Design and implement a security policy for an organisation.**

|  |
| --- |
| <https://github.com/LBruni98/Reboot-Games-Security-Policy/blob/master/README.md#reboot-games-security-policy> |
| The link is to the whole Reboot Games security policy, the document goes in depth about the security that is enforced in the company, Reboot Games. The sections in the document adhere to a typical security policy. The Outline of the business is covered in the ‘Introduction’ section, detailing who the company is and what they do, with the structure of the company, such as listing the employees and how we work within the organisation. Risk assessment is included with the risks and the procedures to prevent them. Security Procedures are covered, noting what the employees must do when entering the building or logging in onto a computer, which are part of the procedures. Data protection is covered with compliance and the process carried out. A disaster recovery plan is noted in case of disaster and what is to be done during this phase. |

**P8 List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion.**

|  |
| --- |
| <https://github.com/LBruni98/Reboot-Games-Security-Policy/blob/master/README.md#9-disaster-recovery-plan> |
| The link above takes the user to the last section of the policy README document. This section details the main components in a disaster recovery plan and explaining why these components are crucial. This section covers the crucial points of a disaster recovery plan with how they are executed, such as a communications plan for the employees, and how these components can help towards the success of data and system recovery. |

**M1 Propose a method to assess and treat IT security risks.**

|  |
| --- |
|  |
|  |

**M2 Discuss three benefits to implement network monitoring systems with supporting reasons.**

|  |
| --- |
|  |
|  |

**M3 Summarise the ISO 31000 risk management methodology and its application in IT security.**

|  |
| --- |
| <https://github.com/LBruni98/Reboot-Games-Security-Policy/blob/master/README.md#41-iso-31000> |
|  |

**M4 Discuss possible impacts to organisational security resulting from an IT security audit.**

|  |
| --- |
|  |
|  |

**M5 Discuss the roles of stakeholders in the organisation to implement security audit recommendations.**

|  |
| --- |
|  |
|  |

**D1 Investigate how a ‘trusted network’ may be part of an IT security solution.**

|  |
| --- |
|  |
|  |

**D2 Consider how IT security can be aligned with organisational policy, detailing the security impact of any misalignment.**

|  |
| --- |
|  |
|  |

**D3 Evaluate the suitability of the tools used in an organisational policy.**

|  |
| --- |
|  |
|  |