**Security (Advocate: Manish Gadhvi)**

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

|  |
| --- |
| <https://github.com/MarkB19988/Security#1-types-of-security-risks-to-organisations>  **COMPLETED** |
| This link points to a section of my Reboot Games security policy document that talks about different types of security risks and groups them into physical risks and computer related risks. |

**P2 Describe organisational security procedures.**

|  |
| --- |
| <https://github.com/MarkB19988/Security#2-reboot-games-organisational-security-procedures>  **COMPLETED** |
| This link points to a section of my Reboot Games security policy that outlines the companies security procedures for different events such as report suspicious activity or simply the process of entering and leaving the building. |

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

|  |
| --- |
| <https://github.com/MarkB19988/Security/blob/master/README.md#3-configuration-of-firewall-policies-and-third-party-vpns>  **COMPLETED** |
| This link points to a section of my Reboot Games security policy that talks about the consequences of having an incorrectly configured firewall or VPN |

**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/MarkB19988/Security#4-how-can-implementing-a-dmz-static-ip-nat-improve-security>  **COMPLETED** |
| This link points to a section of my Reboot Games security policy that explains how implement a DMZ, static IP and NAT can improve the network security of Reboot Games. |

**P5 Discuss risk assessment procedures.**

|  |
| --- |
| <https://github.com/MarkB19988/Security/blob/master/README.md#5-reboot-games-risk-assessment> |
| This link points to a section of my Reboot Games security policy that outlines different potential risks to Reboot Games and explains what can be done to minimize the risk or how to recover if the specified event was to occur. |

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

|  |
| --- |
| <https://github.com/MarkB19988/Security#6-data-protection-process-and-regulations>  **COMPLETED** |
| This link points to a section of my Reboot Games security policy that outlines what data protection rules and regulations Reboot Games has to follow and the process that will be used to ensure that Reboot Games follows these rules and regulations. |

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

|  |
| --- |
| <https://github.com/MarkB19988/Security#reboot-games-security-policy>  **COMPLETED** |
| This link points to the entirety of my Reboot Games security policy. |

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

|  |
| --- |
| <https://github.com/MarkB19988/Security/blob/master/README.md#8-main-components-of-the-organisational-disaster-recovery-plan>  **COMPLETED** |
| This link points to a section of my Reboot Games security policy that outlines what a disaster recovery plan is, what is included in it and what types of potential disasters Reboot Games could face. |

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

|  |
| --- |
| Please use this section to provide all appropriate, valid and checked http Links that point to your evidence; use multiple lines to separate multiple links |
| Please provide a short (between 3 to 8 well considered, fully proofread and reflected sentences) explanation that justifies why the evidence/links you have provided is suitable as evidence of this requirement |

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

|  |
| --- |
| Please use this section to provide all appropriate, valid and checked http Links that point to your evidence; use multiple lines to separate multiple links |
| Please provide a short (between 3 to 8 well considered, fully proofread and reflected sentences) explanation that justifies why the evidence/links you have provided is suitable as evidence of this requirement |

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

|  |
| --- |
| Please use this section to provide all appropriate, valid and checked http Links that point to your evidence; use multiple lines to separate multiple links |
| Please provide a short (between 3 to 8 well considered, fully proofread and reflected sentences) explanation that justifies why the evidence/links you have provided is suitable as evidence of this requirement |

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

|  |
| --- |
| Please use this section to provide all appropriate, valid and checked http Links that point to your evidence; use multiple lines to separate multiple links |
| Please provide a short (between 3 to 8 well considered, fully proofread and reflected sentences) explanation that justifies why the evidence/links you have provided is suitable as evidence of this requirement |

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

|  |
| --- |
| Please use this section to provide all appropriate, valid and checked http Links that point to your evidence; use multiple lines to separate multiple links |
| Please provide a short (between 3 to 8 well considered, fully proofread and reflected sentences) explanation that justifies why the evidence/links you have provided is suitable as evidence of this requirement |

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

|  |
| --- |
| Please use this section to provide all appropriate, valid and checked http Links that point to your evidence; use multiple lines to separate multiple links |
| Please provide a short (between 3 to 8 well considered, fully proofread and reflected sentences) explanation that justifies why the evidence/links you have provided is suitable as evidence of this requirement |

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

|  |
| --- |
| Please use this section to provide all appropriate, valid and checked http Links that point to your evidence; use multiple lines to separate multiple links |
| Please provide a short (between 3 to 8 well considered, fully proofread and reflected sentences) explanation that justifies why the evidence/links you have provided is suitable as evidence of this requirement |

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

|  |
| --- |
| Please use this section to provide all appropriate, valid and checked http Links that point to your evidence; use multiple lines to separate multiple links |
| Please provide a short (between 3 to 8 well considered, fully proofread and reflected sentences) explanation that justifies why the evidence/links you have provided is suitable as evidence of this requirement |