**Security (Advocate: Manish Gadhvi)**

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

|  |
| --- |
| Link: <https://github.com/matthewsides/RebootGames-Policies-And-Procedures/blob/master/README.md#4-risks> |
| The evidence for this criterion may be found in the Reboot Games Policies and Procedures repository and constitutes as meeting the criteria as the general types of security risks to organisations have been identified and explained (Physical risks, Internal, External, Software based, Social engineering, Human risks). |

**P2 Describe organisational security procedures.**

|  |
| --- |
| Link: <https://github.com/matthewsides/RebootGames-Policies-And-Procedures/blob/master/README.md#security-procedures> |
| This is evidenced on GitHub in the Reboot Games Policies and Procedures repository's readme.md. The criteria have been met as security procedures have been defined and illustrated through the designed reboot games procedures for awareness, Use of identity cards and remote access. |

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

|  |
| --- |
| Link: <https://github.com/matthewsides/RebootGames-Policies-And-Procedures/blob/master/README.md#firewall-policies-configuration-issues> |
| This is evidenced on GitHub in the Reboot Games Policies and Procedures repository's readme.md. This criterion has been achieved as the firewall has been briefly defined and the issues of incorrect configuration of firewall policies covered also stating the factors to be considered in relation to Reboot Games when setting up a firewall for a network. Third party VPN's issues have also been addressed, noting the problems of off grounds systems accessing the internal network. |

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

|  |
| --- |
| Link: <https://github.com/matthewsides/RebootGames-Policies-And-Procedures/blob/master/README.md#dmz> |
| The evidence for this criterion may be found in the Reboot Games Policies and Procedures repository. This constitutes as meeting the criteria as how implementing a DMZ, static IP and NAT in a network can improve Network Security has been addressed with the example being in relation to possibly implementing them to Reboot Games. |

**P5 Discuss risk assessment procedures.**

|  |
| --- |
| Link: <https://github.com/matthewsides/RebootGames-Policies-And-Procedures/blob/master/README.md#risk-assessment-1>  <https://github.com/matthewsides/RebootGames-Policies-And-Procedures/blob/master/README.md#risk-assessment> |
| This is evidenced on GitHub in the Reboot Games Policies and Procedures repository's readme.md. Risk assessment is explained with regards to health and safety in an organisations environment and also with regards to data. Whilst procedures in how to prevent risks or mitigate have been outlined, thus meeting this criterion. |

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

|  |
| --- |
| Link: <https://github.com/matthewsides/RebootGames-Policies-And-Procedures/blob/master/README.md#data-protection-policy> |
| The evidence for this criterion can be found in the Reboot Games policies and procedures repository 's readme.md. This is applicable to the criteria as the Mis-use act, Data protection act and more specifically a recently enacted sub set of the act the General data protection regulation has been explained and applied to the Organisation (Reboot Games). |

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

|  |
| --- |
| Link: <https://github.com/matthewsides/RebootGames-Policies-And-Procedures/blob/master/README.md#1-introduction> |
| Evidenced in the Reboot Games policies and procedures repository 's readme.md and achieved as a security policy has been designed and implemented or applied to an organisation (which in this instance is Reboot Games) to ensure the protection of intellectual property and data, etc. |

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

|  |
| --- |
| Link: <https://github.com/matthewsides/RebootGames-Policies-And-Procedures/blob/master/README.md#9-disaster-recovery-plan> |
| The evidence for this criterion can be found in the Reboot Games policies and procedures repository 's readme.md. This criterion has been met as the components of an organisational recovery plan have been outlined and justified for the reasons for inclusion (backups, communication plan, role assignments, data continuity system, etc.). |

**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 |
| Disaster recovery plan, what do you do if something goes wrong. Go look at examples in organisations and find what’s reasonable. What do you denote (deem) as a disaster? What you need to do to recover from / need to figure out what to do. Need to have a good understanding of your organisation. Must state why your risk is important to your organisation. All about knowing the organisation.look at where we are geographic, what we do, the people in the company. |

**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 |