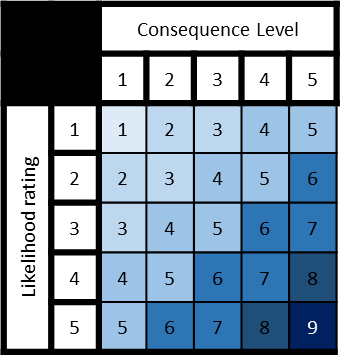
**Risk Matrix**

The risk assessment uses a risk matrix. To help quickly understand how important it is to minimise the risk, an evaluation on likelihood and consequence (lower numbers for less likelihood and smaller consequences) is entered in the following table and the given is categorised as below:



Key: (Value – Category of Risk)

1 = Negligible risk

2-3 = Minor risk

4-5 = Moderate risk

6-7 = Strong risk

8 = Major risk

9 = Critical risk

**Risk Assessment Table**

Potential risks to the project all have a category and have a prepared mitigation to prevent them from occurring and give direction for if they occur.

|  |  |  |  |
| --- | --- | --- | --- |
| Hazard and Category | | Risk Specifics | Measures |
| Electrical Hazards | Minor (1-3) | Damaged or badly managed electronics can pose an electrical hazard to workers. | - Do not use Damaged or faulty equipment, especially if there are exposed wires.  - Tell others in the vicinity about the hazard and the proper persons to get the equipment replaced or fixed.  - Keep drinks and other liquids out of areas with electronic equipment. |
| Physical Effects of Computer Use | Moderate (4-2) | Workers spending a lot of time on a computer may experience some of the following negative consequences:  - Eye tiredness and strain  - Back and posture pain  - Repetitive strain injury | - Take regular breaks when working which include not just looking away from the screen but standing and moving the body.  - Keep screen brightness to the lowest usable option and when working late use software to reduce blue light.  - Have supportive chairs have workers sit properly in them, a proper distance away from the screen. |
| Equipment Security | Moderate (1-5) | Loss of the physical equipment and all hard data due to crime or disaster (fire, flood). | -Have a secure office place only accessible to those with the correct authority (e.g. lock doors, do not allow in random people).  - Have working fire alarms and have workers know emergency numbers. |
| Data Security | Strong (2-5) | This involves data collected from users being compromised. | - Store data in a secure location and always require passwords to access data.  - Minimise amount of locations data is saved.  - Do not store data portably.  - If physical copies of data are made, ensure they are properly destroyed when no longer needed.  - Ensure there is encryption and pseudonymization of data. |
| User Safety | Moderate (1-4) | Users may contact other users, and some may have malicious intentions. | - Have reminders to users about how to keep themselves safe (meet in neutral locations and inform a trusted person etc.)  - Require verification steps to create an account including (but not limited to) captchas and institution verification.  - Option to anomalously report suspicious or malicious users to be reviewed by a real person. |
| Data Loss | Strong (2-5) | Nodes/servers in the data storage centre may go down, therefore losing data about users and/or projects. | - Make use of server provider’s data replication services to ensure automatic backing up of data held (e.g. data redundancy packages). |