RISK REGISTER

Risk Description *Brief description of risk*	Probability Score *1-5 based on matrix*	Impact Score *1-5 based on matrix*	Severity Score *Severity = Probability + Impact*	Choose Strategy : • *Avoid* • *Reduce* • *Transfer* • *Accept*	Actions to be taken to mitigate the risk
1 A breach of *security and/or protocol compliance* **while working in a home office.**	1	3	4	Reduce	All staff trained and cautioned to only use Gelos-provided equipment and data sharing software to avoid accidental breaches of compliance.
2 A breach of *security and/or protocol compliance* **while working in a café**.	3	4	7	Avoid	Staff are cautioned to avoid working in a publicly shared spaces on Gelos-related projects. Infringements of this (Tracked via security suite software) are penalised.
3 A breach of *cyber security guidelines* **when working on emails**.	3	2	5	Accept	Accidental infringement of client data is almost a certainly in the course of

Risk Description ***Brief description of risk***	**Probability Score** ***1-5 based on matrix***	**Impact Score** ***1-5 based on matrix***	**Severity Score** ***Severity = Probability + Impact***	**Choose Strategy :** • ***Avoid*** • ***Reduce*** • ***Transfer*** • ***Accept***	**Actions to be taken to mitigate the risk**
					carrying out work. Gelos will do its best to ensure all staff are trained and aware of client-data practices.
4 A breach of *security and/or protocol compliance* **by a contractor**.	4	5	9	Transfer	Gelos will ensure that any breaches are settled by the contractor's insurance policy(ies), and cooperate with any legal investigations and inquiries.
5 Employee remote-working opening a spam email that has the potential to infect Game Environment player database.	4	4	8	Reduce	Adapt polices and procedures to include clauses toward **limiting** the opening of whitelisted third-party emails with offending employees
6 Employee unknowingly disclosing player personal	2	5	7	Accept	The severity of this reflects badly not only on Gelos itself, but erodes any trust our consumers or partners have

Risk Description *Brief description of risk*	Probability Score *1-5 based on matrix*	Impact Score *1-5 based on matrix*	Severity Score *Severity = Probability + Impact*	Choose Strategy : • *Avoid* • *Reduce* • *Transfer* • *Accept*	Actions to be taken to mitigate the risk
details in an email to external party					in us and our services. Therefore, this employee would need to be released contractually from service.

Risk Matrix

	Impact (right)	Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood (below)	Rating (below and right)	1	2	3	4	5
Almost certain	5	6	7	8	9	10
Likely	4	5	6	7	8	9
Possible	3	4	5	6	7	8
Unlikely	2	3	4	5	6	7
Rare	1	2	3	4	5	6

Additional Information

1) For each of the four risks, what could be affected by this risk, including issues relating to IP, Ethics and Privacy.

For the first risk, the probability for a risk to occur is not significantly high, and any breach is very likely to be internal amongst staff. While an issue of ethics, provided staff training and non-disclosure agreements from all Gelos staff satisfies any risk factors.

To the second risk, there is a much higher occurrence chance of breach while working in a public space, and the impact would be far higher as the breach would open client/project details to the public face. It is best to be overly cautious in this regard and prevent any such breach from happening in the first place.

On the third risk, breaches while writing an email are possible if staff are not aware to whom emails are addressed to or else are being included in CC; or BC; lines. Given that this is an internal breach, the impact of this is low, for the same reasons as the first risk.

Finally to mention the fourth risk, the risk probability of a contractor carrying out duties on behalf of Gelos is incredibly high as there is no realistic way to fully monitor or closely scrutinise the procedures or methods of such external personnel. A data breach in this way is likely to be very catastrophic, as Gelos has no way of knowing where the data has ended up, and is very unlikely to have any control over the third-parties that could be involved.

2) How could you track the effectiveness of the risk management strategies. Suggest a benchmark or indicator you could use to assess how effective each strategy is.

Keeping an incident log for any breaches that occur will help to ensure that not only are incidents known about and tracked, but that they are accurately classified in the RACI both in terms of accuracy, and in how that style of breach has affected Gelos with historical data and evidence.

3) What feedback processes would you recommend for providing warning of new risks?

An open-communication policy across all levels of staff will help enable the identification of new potential risks that differing perspectives and insights may offer. Classification and suggestion should be a simple and easy process, so as not to discourage team members from speaking out and offering knowledge and could be critical for the maintenance and management of Gelos' image, reputation, and ethics.

Determine whether staff members are complying with the approved cyber security risk strategies. Review the two incidents (outlined above) and complete the following:

Referring to your cyber security risk management strategies and SOP, analyse whether the employees complied with the strategies and where any non-compliance occurred.

The established management and cyber security risk strategies of Gelos did not account for the incidents in question, and while non-compliance was not committed to the black-and-white letter of the policies, the ethics and general morals sought to be upheld by Gelos and its employees certainly were. The risk register needed to be updated (Risks 5 and 6), to account for the oversights in the original register, with the consequences upheld retroactively.