

Digital Preservation: Risk Mitigation Worksheet

2022

1. How many files do you have?
2. How many MB, GB, TB, etc.?
3. How fast are you digital assets growing? (GB or TB per year)
4. What file types do you have?
5. How are your files stored? (desktop, laptop, network, external hard drive, cloud, etc.)
6. Who manages your digital storage? (you, a colleague, IT person, outsourced, etc.)
7. Who has access to your files? (can impact legal issues, e.g. copyright)
8. Can you restrict access as necessary?
9. Is your virus and malware protection up to date? (if you manage your files)
10. How are your files organized? Does this work, or is change necessary?
11. Are you using good file naming conventions that help provide context and accessibility?
12. Do you have any media at risk of degradation? (delaminating CDRs, old thumb drives, diskettes, etc.)

13. Do you have any obsolete file formats that need migrating to preservation formats?
Use PRONOM database for unknown file types.
<https://www.nationalarchives.gov.uk/pronom/BasicSearch/proBasicSearch.aspx?status=new>

14. Do you run backups? If so, how often?

15. Do you have geographically distant backups? If not, where do you think you could do this?

16. What are the organizational risks to your digital assets? (management turnover, budgets, IT support instability, etc.)

17. Are your digital assets part of your organization's COOP?

18. Are you reevaluating your practices, documentation, hardware, software, etc. annually to make sure they still serve you well?

19. Have you created documentation? *(If not, use your answers above as a great start to capture how you manage and protect your growing, valuable digital assets.)*