The Rockefeller Foundation
420 Fifth Avenue, New York, NY. 10018-2702

Cybersecurity Questionnaire

The intention of this document is to provide The Rockefeller Foundation (RF) with assurance that any confidential data is being secured properly. RF places a high value on cybersecurity and believes this exercise cannot only help protect data related to this grant, but also help to strengthen cybersecurity practices on the whole at your organization.

If there are any significant findings from this document, RF will aim to work alongside the grantee organization to improve their cybersecurity practices.

Please attach any additional documentation you believe may be helpful in responding.

Organization Name & Address
Primary Organization Contact
Cybersecurity Questions
1. As a part of this grant will you be collecting any confidential information? *If yes, please describe the type of data being collected.*
2. What system(s) will be used to collect and transmit the confidential data? *List all tools and related security controls.*
3. What systems will you use to store the confidential data?
4. What controls are in place to protect access to and extraction of confidential data where it is being stored? Is it possible to export /share the data, what controls exist around exports or sharing?

The Rockefeller Foundation
420 Fifth Avenue, New York, NY. 10018-2702

5. Is there any monitoring and logging around access and export of the confidential data?
6. How long will confidential information be kept in your systems? And how is its disposal handled?
7. Will anyone outside of the grantee organization have access to confidential information? *If so, whom? Has a security review been performed on the 3rd party?*
8. What is the information access policy in place at your organization? **Has it been communicated to all employees? How often is it communicated? How often is it reviewed?**
9. What are your password requirements for access to you network and business critical systems? *(E.G., what are the rules for setting – length, alpha numeric. etc., how often do they expire, etc.)*
10. Is remote access to the internal network limited to authorized users? *If so, how is it limited?*
11. Do the systems where you are storing the data require two-factor authentication (2FA)? Specifically, do you require 2FA on email, content management, Virtual Private Network (VPN)access and/or financial systems?

The Rockefeller Foundation
420 Fifth Avenue, New York, NY. 10018-2702

12. Have you ever had a security breach:
- **a) that resulted in data being stolen or in data being damaged, altered or**
- **b) deleted or that required notification under privacy laws?**

If so, what corrective measures were put in place to avoid a future breach?

13. What security applications are in place to protect email?

14. Do you have periodic network penetration testing and/or security audit performed by an independent entity?

If so, when was the last penetration testing and what were the results? Please provide an executive summary.

15. Does your organization have a formal process for developing and maintaining business continuity?

16. Does your organization have a documented information security incident response procedure?

If so, how often is it reviewed?

17. Does your organization provide cybersecurity training for employees and consultants?

If yes, please describe.

18. Are staff and consultants required to use a company desktop, laptop, or mobile device when accessing company data and services? Please describe how all company endpoints are secured.
19. If you allow "Bring Your Own Devices" (BYOD), how are you protecting organizational information?
20. Please list any additional security tools and devices that you have in place at your organization and how they are being used.
21. Are company devices secured using firewall, antivirus or edr to enforce security controls?
22. How often are patches or system updates deployed to workstations and servers?