100 Point Cyber Controls

I. Cybersecurity Policy and Governance (Points 1-10)  
  
1. Establish a dedicated cybersecurity team.  
2. Develop a comprehensive cybersecurity policy.  
3. Define roles and responsibilities for cybersecurity within the organisation.  
4. Establish a governance structure for cybersecurity oversight.  
5. Conduct regular cybersecurity risk assessments.  
6. Develop a cybersecurity awareness training program.  
7. Implement an incident response plan.  
8. Establish a protocol for reporting security incidents.  
9. Regularly review and update cybersecurity policies and procedures.  
10. Ensure compliance with relevant laws and regulations.

II. Employee Training and Awareness (Points 11-20)  
  
11. Conduct regular cybersecurity awareness training for all employees and volunteers.  
12. Provide specific training for employees with elevated access privileges.  
13. Educate staff about social engineering threats like phishing attacks.  
14. Promote a culture of security awareness and vigilance.  
15. Provide resources and materials to reinforce cybersecurity education.  
16. Conduct simulated phishing exercises to test employee awareness.  
17. Encourage reporting of suspicious activities without fear of reprisal.  
18. Recognise and reward employees for their cybersecurity efforts.  
19. Establish a process for continuous cybersecurity education and training.  
20. Provide clear guidelines on acceptable device usage and security practices.

III. Access Control and Identity Management (Points 21-30)  
  
21. Implement strong password policies.  
22. Encourage the use of password managers.  
23. Enable multi-factor authentication for all accounts.  
24. Regularly review and update user access privileges.  
25. Implement the principle of least privilege.  
26. Conduct regular access reviews.  
27. Disable inactive accounts promptly.  
28. Implement a secure process for user onboarding and offboarding.  
29. Limit physical access to sensitive areas and systems.  
30. Regularly update and patch all software and systems.

IV. Data Protection and Encryption (Points 31-40)  
  
31. Encrypt sensitive data at rest.  
32. Encrypt data transmitted over networks.  
33. Implement data loss prevention measures.  
34. Define and classify different types of data (public, internal, confidential).  
35. Ensure secure storage and transmission of financial data.  
36. Regularly backup critical data and establish a disaster recovery plan.  
37. Monitor and restrict the use of removable media devices.  
38. Implement secure file sharing and collaboration tools.  
39. Develop a secure data disposal policy.  
40. Train employees on handling and protecting sensitive data.

V. Network Security (Points 41-50)  
  
41. Implement a robust firewall and intrusion detection system.  
42. Regularly update antivirus and anti-malware software.  
43. Secure Wi-Fi networks with strong encryption.  
44. Segment the internal network to limit lateral movement in case of a breach.  
45. Implement DNS filtering to block malicious websites.  
46. Establish VPN access policies for remote workers.  
47. Regularly conduct vulnerability assessments and penetration testing.  
48. Implement network logging and monitoring.  
49. Develop a network security policy for remote workers.  
50. Establish procedures for secure mobile device usage.

VI. Vendor and Third-Party Risk Management (Points 51-60)  
  
51. Identify and categorise third-party relationships.  
52. Evaluate the cybersecurity posture of third-party vendors.  
53. Include cybersecurity requirements in vendor contracts.  
54. Regularly monitor third-party compliance with cybersecurity standards.  
55. Establish procedures for securely exchanging information with third parties.  
56. Develop incident response plans with key vendors.  
57. Regularly review and update vendor agreements.  
58. Educate employees about the risks associated with third-party services.  
59. Implement controls for third-party access to sensitive data.  
60. Establish a process for promptly revoking third-party access upon contract termination.

VII. Physical Security (Points 61-70)  
  
61. Implement access controls for physical premises.  
62. Install security cameras and alarms in sensitive areas.  
63. Regularly audit physical access logs.  
64. Secure laptops and mobile devices with tracking and remote wipe capabilities.  
65. Implement visitor logs and escort procedures for non-employees.  
66. Train employees on physical security best practices.  
67. Securely store keys, access cards, and other physical access credentials.  
68. Implement secure disposal procedures for physical documents and devices.  
69. Conduct periodic physical security assessments.  
70. Regularly update physical security policies and procedures.

VIII. Incident Response and Recovery (Points 71-80)  
  
71. Develop an incident response team and assign specific roles.  
72. Establish communication protocols during a security incident.  
73. Develop a detailed incident response plan covering various scenarios.  
74. Regularly conduct tabletop exercises to test the incident response plan.  
75. Establish relationships with external cybersecurity experts for incident response support.  
76. Document lessons learned from security incidents and near misses.  
77. Develop a business continuity plan in case of a prolonged cybersecurity incident.  
78. Regularly update incident response and recovery procedures.  
79. Establish a process for reporting incidents to regulatory bodies.  
80. Engage in public relations and communication efforts during a significant incident.

IX. Legal and Compliance (Points 81-90)  
  
81. Stay updated with relevant cybersecurity laws and regulations.  
82. Establish a legal response team for cybersecurity incidents.  
83. Document and retain evidence related to security incidents.  
84. Regularly audit and document compliance with relevant regulations.  
85. Develop procedures for handling legal requests for information.  
86. Engage legal counsel experienced in cybersecurity matters.  
87. Regularly review and update legal and compliance procedures.  
88. Establish a process for reporting breaches to affected individuals and authorities.  
89. Develop procedures for international data transfers in compliance with regulations.  
90. Engage in regular legal training for staff involved in cybersecurity matters.

X. Continuous Improvement and Innovation (Points 91-100)  
  
91. Establish a cybersecurity innovation team to explore emerging technologies.  
92. Regularly review emerging threats and adjust security measures accordingly.  
93. Encourage employees to propose cybersecurity improvement ideas.  
94. Regularly engage in threat intelligence sharing with other organisations.  
95. Establish a cybersecurity research and development fund.  
96. Regularly participate in cybersecurity conferences and workshops.  
97. Collaborate with academia and research institutions on cybersecurity initiatives.  
98. Establish a bug bounty program to incentivise security researchers to identify vulnerabilities.  
99. Regularly assess the effectiveness of cybersecurity training programs.  
100. Recognise and celebrate cybersecurity achievements and milestones.