Date: [Insert Date]

To: [Insurance Carrier Name]
Attn: Underwriting Department
Policy Number: [Insert Policy Number if applicable]

Subject: Statement of Ransomware Defense and Cyber Security Controls

Dear Underwriting Team,

This letter serves to formally outline the ransomware defense protocols and cybersecurity controls currently implemented at [Company Name]. We understand the evolving threat landscape and have prioritized the following measures to mitigate risk:

1. Authentication and Access Control
We have implemented Multi-Factor Authentication (MFA) across all remote access points, administrative accounts, and cloud-based email services. We follow the principle of least privilege (PoLP) for all user permissions.

2. Backup and Recovery
Our organization maintains encrypted, off-site, and air-gapped backups of mission-critical data. We perform regular restoration tests to ensure a Recovery Time Objective (RTO) of [Insert Timeframe].

3. Endpoint Protection
All workstations and servers are protected by an Endpoint Detection and Response (EDR) solution that is monitored [24/7 / regularly]. Patch management protocols ensure that critical security updates are applied within [Number] days of release.

4. Email Security and Training
We utilize advanced email filtering to block malicious attachments and phishing attempts. Furthermore, all employees undergo mandatory security awareness training and simulated phishing tests on a [Monthly/Quarterly] basis.

5. Incident Response
[Company Name] maintains a formal Incident Response Plan (IRP) specifically addressing ransomware scenarios. This plan is reviewed and updated annually.

We believe these controls demonstrate our commitment to maintaining a robust security posture. Please let us know if you require additional documentation or a technical walkthrough of our environment.

Sincerely,

[Signature]
[Name of Authorized Representative]

[Title, e.g., CTO / CISO / IT Director]
[Company Name]