NYC Mesh Services Security Policy

- All data on production Mesh Services shall be encrypted at rest with strong encryption as defined by NIST SP 800-175B. Production Mesh Services handling member data should use AES with the key size of 256 bits.
- All backups from production Mesh Services shall be encrypted at rest with strong encryption as defined by NIST SP 800-175B. Production Mesh Services handling member data should use AES with the key size of 256 bits.
- Network traffic involving production Mesh Services and passing data over public networks shall be encrypted with strong encryption as defined by NIST SP 800-175B.
- Logs, backups, and member data shall be retained and destroyed in accordance with local, state, and national laws.
- All production Mesh Services shall be protected by discrete or host based firewalls.
- Firewall rules shall expose the minimum viable subset of possible ports to enable successful operation of the service.
- No firewall rules applied to production Mesh Services shall contain ANY as the source or destination zones.
- Unused firewall rules shall be removed when no longer required.
- Firewall rules protecting production Mesh Services shall be periodically reviewed by service owners and the NYC Mesh Maintenance Team to ensure only required rules are retained.
- All services hosting production Mesh Services shall install, enable, and monitor intrusion detection and prevention systems.
- All logs and alerts from configured intrusion detection and prevention systems shall be reviewed and retained by the NYC Mesh Net SOC.