General Security Policy – Morris-Taylor Household & Homelab

Policy ID: GSP-001

Effective Date: April 19, 2025

Review Cycle: Annually (From Effective Date)

Owner: Grayson – Security Administrator

Version: 1.0

1. Purpose

The purpose of this policy is to define the general security expectations and baseline safeguards for all systems, devices, and data within the Morris-Taylor household and homelab environment. This policy also outlines responsibilities and rules to ensure the safety, privacy, and availability of digital and physical assets for all household members. For this purpose of this document household members refer to individuals that regularly reside at the home's listed address, guests refer to any individual invited into the household for brief visitation, users refer to any individual using computing or digital resources owned by households' members, and administrators refer to the two heads of household (Kari and Grayson)

2. Scope

This policy applies to:
- All physical devices (PCs, laptops, tablets, smartphones, IoT, home server, etc.)
- All virtual infrastructure (VMs, containers, cloud services)
- All household members, guests, and future dependents
- All data handled within or across the homelab/home network

3. Guiding Principles

- Confidentiality: Sensitive information must be protected from unauthorized access via methods of encryption, obfuscation, hashing, or other means of making data non-readable.
- Integrity: All systems and data must be accurate and protected from unauthorized modification, any modifications must be documented via logging or verbal permission.
- Availability: Critical systems and data must be reliably accessible to authorized users and guests, goal of 99.99% uptime is to be achieved in a calendar year.

- Resilience: Plans must exist to recover from disruptions and incidents as quickly as possible.

4. Responsibilities

Role	Responsibility
Grayson (Security Admin)	Maintain homelab, perform regular audits, manage backups, enforce policies, perform regular patching, update policies and procedures, ensure uptime
Fiancée (User/IT Admin)	Follow security practices, report issues, participate in drills and reviews, ensure adherence to policies and procedures set forth in this, and following documentation.
Future Children	Follow age-appropriate tech rules, respect device usage boundaries, and time limits
Guests	Use only the Guest VLAN/Wi-Fi, no access to internal resources or admin systems

5. Device Security Requirements

- All end-user devices must have full-disk encryption enabled (BitLocker, LUKS, etc.).
- Devices must auto-lock after 10 minutes of inactivity.
- All systems are required to maintain the latest versions of operating systems and installed software.
- Only approved devices may access internal VLANs or trusted systems.
- Root/admin access is restricted to Grayson and Kari unless explicitly delegated via written or verbal permission.

6. Network & Access Controls

- Separate VLANs for trusted devices, IoT, guests, and lab environments.
- Strong WPA3 password for primary Wi-Fi; guest network on WPA2 with time limits.
- Firewall rules must enforce east-west segmentation between VLANs.
- Remote access (e.g., VPN, SSH) requires MFA, baseline security, and certificate-based authentication.

7. Passwords & Authentication

- All critical accounts must use MFA (TOTP or hardware token preferred).
- Passwords must be at least 14 characters and stored in a password manager (e.g., Bitwarden).
- Shared credentials (e.g., for media services) must be rotated every 9 months.

8. Logging & Monitoring

- All homelab systems log auth events, network activity, and system changes.
- Logs must be forwarded to a central logging solution and retained for 6 months.
- Alerting is configured for suspicious activity or multiple failed login attempts.

9. Backup & Recovery

- Key systems (NAS, VMs, important documents) are backed up weekly to an external encrypted drive and cloud storage.
- Offsite backups are created and rotated to a location separated by at least 120 geographical miles. Offsite backups will be tested monthly during drive rotations.
- All backups are encrypted at rest and in transit.

10. Change Management

- A management policy will be implemented and enforced.
- All changes will be to systems including configurations, software installation, etc. will be documented and handled by a designated change owner.
- In the event of a failed change the Backup and Recovery Plan will be activated and appropriate measures taken to minimize downtime

11. Policy Violations

Any violation of this policy may result in restricted access to systems or devices. Exceptions must be documented and reviewed annually.

12. Annual Review

This policy must be reviewed and updated each calendar year according to effective date to reflect changes in technology, threat landscape, and household needs. A detailed security assessment and capacity planning assessment will be performed with the annual review and updates to this document reflected accordingly.

Signed:

Recoverable Signature

X Grayson Morris

Grayson Morris
Security Administrator
Signed by: 53276d7a-600c-4b1b-a62d-b07ae6f4ca9d