**PROJECT: STEP BY STEP GUIDE TO PERSONAL CYBER HYGIENE AUDIT**

**I.** **Password Management**

1. **Password complexity**: Review your passwords for strength and complexity. Ensure they contain a mix of uppercase and lowercase letters, numbers, and special characters.

2. **Password uniqueness**: Verify that you're using unique passwords for each account. Avoid reusing passwords across multiple sites.

3. **Password manager**: Consider using a reputable password manager to securely store and generate strong passwords.

**II. Device Security**

1. **Operating system updates**: Ensure your devices (computers, smartphones, tablets) are running the latest operating system versions.

2. **Antivirus software**: Install and regularly update antivirus software on your devices.

3. **Firewall configuration**: Verify that your device firewalls are enabled and properly configured.

**III. Account Security**

1. **Multi-factor authentication** (MFA): Enable MFA whenever possible, especially for sensitive accounts (e.g., email, banking, social media).

2. **Account monitoring**: Regularly review your account activity and transaction history to detect potential security issues.

3. **Account closure**: Identify and close unused or unnecessary accounts to reduce your attack surface.

**IV. Online Behavior**

1. **Phishing and spam awareness**: Be cautious when receiving unsolicited emails or messages, and avoid clicking on suspicious links or providing sensitive information.

2. **Public Wi-Fi usage**: Limit your use of public Wi-Fi networks, and consider using a virtual private network (VPN) when connecting to public networks.

3. **Software downloads**: Only download software from reputable sources, and be wary of free or pirated software.

**V. Data Backup and Storage**

1. **Regular backups**: Ensure you're regularly backing up your important data to a secure location, such as an external hard drive or cloud storage service.

2. **Data encryption**: Consider encrypting sensitive data, both in transit and at rest.

3. **Cloud storage security**: Review the security settings and access controls for your cloud storage accounts.

**VI. Review and Revision**

1. **Regularly review**: Schedule regular reviews of your personal cyber hygiene (e.g., every 3-6 months).

2. **Revise and improve**: Based on your review, revise and improve your cyber hygiene practices as needed.

By following these steps, you'll be able to identify potential vulnerabilities, adopt best practices, and reinforce a proactive security mindset to protect your digital life.