|  |  |
| --- | --- |
| App Full Title | Internet of Things (IoT) Security Best Practices by UTM |
| App Short Title | IoT Security UTM |
| Target Device | Smartphones |
| Target Users | [Focused] SMEs’ Employees  [General] Public |
| Purpose | To provide reference for users on general safeguards on IoT Devices |
| Interface Requirement (description) | Easy to navigate through touching interested topic sentences that immediately opens up the contents. |
| Additional Requirement | Able to be used without internet connection. \*contents are fully downloaded upon app installation\* |

[ ] – instructions / direction for developer

( ) - explanations

Design suggestions:-

Welcome screen [generally]:

1. IoT Security Best Practices
2. Home button
3. Scroll down to show more contents [title sections hyperlinked], can be also designed using side-bar pop-out.
4. [optional] settings to allow user-customized reading design (adjust font size, dark mode)

Between screens:

1. Home button to return to main page
2. Display the user chosen title contents
3. Scroll to read more

--- continue to next page for contents ---

Internet of Things (IoT) Security Best Practices

Topics with sub-topics [to be used as structuring the design, user will choose one of the topics to display the sub-topics then again choose the sub-topics to display content, if no sub-topics, then proceed to show contents]:

1. Asset Protection
   1. Physical protection
   2. Establishing & Maintaining Identities / Access Control
   3. Compliance Management
   4. Data / Information Protection Model & Policy
2. Third-Party Management
   1. Product Supply Chain Management
   2. Legal & Third-Party Services Dependencies Management
3. Operation and Maintenance
4. Monitoring and Incident Management

*Contents to be displayed upon user’s choice [refer to the above section for navigation based on bolded text]*

Best Practices for **Physical Protection** in IoT:

1. Inventory Everything
   * Produce a comprehensive document that lists all IoT devices that belongs to the company with respective user’s work ID
2. Do not network if you do not have to
   * Work without connecting to the internet if not required as this would help decrease the threat exposure of the device.
3. Secure the human-layer
   * Ensure that the user’s ID understands the company’s policy of using company’s properties (IoT devices) and it should be taken care properly while periodically maintained by responsible department.
4. Update devices regularly
   * User should be notified for device’s update when it is required and enforce it if there is security issue such as prevent operability unless updated by responsible department then release.
5. Monitor systems in real-time
   * IoT devices connect to the internet most of the time which enables for it to be monitored on its condition and it should alert should there be an issue with it through the server protection architecture.
6. Improve management of your mobile IoT Devices
   * Not all IoT devices needs to be used at once and unused device should be promptly returned to responsible department for safekeeping, user should be alerted when the device has been offline for a duration that is considered to be “too long”.

--- continue to next page for contents ---

Best Practices for **Establishing & Maintaining Identities / Access Control** in IoT:

1. Have strong and precise passwords
   * The standard password has increased a lot that the minimum requirements for it now is 1 lowercase letter, 1 upper case letter, 1 symbol and must be of certain length (8 is recommended which is not too short for security and too long to remember).
2. Safeguarding your records
   * Keep a document that logs the IoT device’s activity in a separate folder which has a certain layer of security that only allows certain users to access.
3. Multi-component authentication
   * Add another password feature for verification on IoT device (usually named as Multi-Factor Authentication) and best is biometric when possible as no two individuals have similar biometric structure.
4. Apply a VPN for connectivity through wireless
   * VPN isolates your network activity from being easily accessed through internet which helps to prevent accidental information leaks when connected to a public / home network.
5. Always encrypt sensitive information
   * Encryption is another password security feature which helps to randomized the password logs on the device which prevents threat actors from obtaining the device’s password easily.

Best Practices for **Compliance Management** in IoT:

1. Admins must have all visibility into all connected devices
   * It is required for company and non-company assets’ information to be logged when it attempts to connect to the company’s network as this would help to filter unwanted connections.
2. Real-time reporting for all devices
   * IoT devices connected to network should show-up in device management logs in order to ensure the device is used properly and within its limited operations.
3. Automation of operational tasks
   * Tasks that are simple and repeated should be automized to prevent any anomalies from occurring during normal operation.

--- continue to next page for contents ---

Best Practices for **Data / Information Protection Model and Policy**:

1. Apply flexible, secure and complex password
   * Password requirements should not be limited to only letters as this would make it easier for threat actors to gain access with reduced time spent for cracking.
2. Apply encryption for authentication
   * Multiple security layers are not fool-proof but it would considerably increase the time spent by threat actors to gain authentication.
3. Build application using latest security standard and protocols
   * Latest security standard needs to be adhered as this would also address newly developed hacking techniques.
4. Apply IoT management platforms
   * IoT device should come with a management center which provides the overview of the device’s security condition.

Best Practices for **Product Supply Chain Management** in IoT:

1. Segmented networks
   * This isolates threats that would come from third-parties / vendors and would also help in accountability of third-parties.
2. Frequent updates
   * Third-party providers should have regular updates required for implementation on devices to ensure their own service and trustfulness.
3. Follow latest security standards
   * Third-party providers should follow the standard security protocols which also helps their company and provided company from being a liability.

Best Practices for **Legal and Third-Party Services Dependencies Management** in IoT:

1. Recent version releases for every component used
   * Third-Party Services should provide the latest version of components which provides better security measures.
2. Identification of new security threats
   * Provided company and third-parties should be aware of latest security threats and address it when required.

--- continue to next page for contents ---

Best Practices for **Operation and Maintenance**:

1. Purchase / Lease IoT equipment from reputable companies
   * Refer to other companies or public reviews when considering an IoT equipment and providing company.
2. Hire a professional for installation
   * Most purchased / leased devices will have a professional installer and if it does not, hire a certified installer or in-house certified installer.
3. Deactivate / Deauthorize unused devices
   * Unused devices need to be deactivated immediately to reduce the threat risk source.
4. Reset device to Factory Default before disposing
   * Factory Default will cause devices to delete all information and data when it was used which ensures that the device’s history cannot be taken advantage of.
5. Regularly update the software in the device
   * Device software updates need to be rolled out to ensure security and operability, it is also done periodically which helps to schedule its operations.
6. Keep your internet connection secure
   * Ensure that provided on-site internet connection is limited to certain criteria to prevent back-tracking by threat actors.

Best Practices for **Monitoring and Incident Management**:

1. Track and manage devices
   * IoT devices can be tracked digitally but it is also a good idea to have manual tracking which can show differences on the device’s condition.
2. Regularly conduct threat exercises
   * Users should be trained at a minimum level to ensure that they would know how to safeguard the device and would refer to responsible department when an issue arises.
3. Segment your network
   * Network segmentation helps to reduce the risk exposures by introducing network complexity to threat actors.

--- end of document ---