City of Albuquerque
Block List Management Standard

ORIGINATION DATE:	1/3/2025
EFFECTIVE DATE:	5/15/2025
VERSION:	1.1
ISSUED BY:	DTI Security
APPROVED BY:	TRC
DATE APPROVED:	5/15/2025

Standard for Block List Management

1. Purpose:
The purpose of this standard is to define the procedures for maintaining, updating, and communicating changes to IT Security Team block lists. These include application block lists (as managed through Unified Endpoint Management [UEM]) and country block lists (implemented through Firewalls). This ensures a consistent approach to address current and emerging threats, while providing transparency and collaboration with DTI stakeholders.

2. Scope:
This standard applies to all DTI Security Team members and any personnel involved in managing or monitoring block lists within the City of Albuquerque's IT environment. The block lists will be maintained and shared on the ISGG intranet website and are accessible to relevant IT employees.

Out of Scope:

- Endpoint Detection and Response (EDR) systems.
- Email-related block lists or filtering mechanisms.
- Any security mechanisms not directly related to UEM or firewall configurations.

3. Definitions:

- **Block List**: A list of applications, countries, or other entities restricted due to security concerns.
- **Change Control Board (CCB)**: A group responsible for reviewing and approving changes within the City's IT environment.
- **Current Threat**: A security issue that poses an immediate risk to the organization's IT systems, networks or data.
- **ISGG**: Information Security Guidance Group, a collaborative IT group involved in developing, refining, and propagation of information security guidelines, standards, and policies tailored to the city's unique challenges and environments.

- **Unified Endpoint Management (UEM)** is a set of tools that enable centralized management, monitoring, and security enforcement across all organization-owned and employee-owned endpoint devices (e.g., desktops, laptops, mobile devices, tablets, IoT).

4. Responsibilities:

- **DTI Security Team**:
    - Maintain and update block lists.
    - Ensure proper documentation of changes.
    - Communicate changes through approved channels.
- **ISGG Members**:
    - Review and provide feedback on block list changes.
    - Disseminate relevant information to their departmental teams.

5. Block List Maintenance Process:

5.1 Creation and Updates:

- **Applications**: Applications flagged as malicious or non-compliant with organizational policies are added to the block list in the UEM platform.
- **Countries**: Countries posing a threat to the organization are added to the firewall block list.

5.2 Approval Process:

- ISGG provides an informal review for communications and raise any exceptions prior to escalation to the CCB.
- Routine updates to block lists shall be approved by the CCB during scheduled meetings.
- Emergency additions due to current threats may bypass the CCB process but require post-event documentation and review at the next CCB meeting.

5.3 Documentation:

- Maintain a centralized repository of block list records on the ISGG intranet website.
- Include details such as:
    - Date of addition/removal.
    - Reason for inclusion/removal.

- Approved by (in case of routine updates).

- Communication of changes to DTI Director Team.

6. Communication of Changes:

6.1 Routine Updates:

- Communicate routine updates through ISGG monthly meetings and/or email.
- Present request for changes during CCB sessions.
- Publish updates on the ISGG intranet site.

6.2 Emergency Changes:

- Notify ISGG members and other relevant IT stakeholders via email with details of the threat and the action taken.
- Update the ISGG intranet site immediately.
- Present the emergency change during the next CCB session for formal review.

7. Threat Response Process:

- Monitor external and internal threat intelligence feeds.
- Assess threats for any changes needed in the block lists.
- Document and provide communication actions taken.

8. Periodic Review:

- Conduct a periodic review of the block lists to ensure accuracy and relevance.
- Review the effectiveness of changes during ISGG meetings and adjust the process as necessary.

9. Enforcement:

Violation of this policy may result in removal of block object management privileges. Additionally, any violation shall be reported to the appropriate supervisor and could be subject to potential disciplinary action, up to and including termination.

City of Albuquerque
Block List Management Standard

10. Exceptions:

Limited exceptions to the policy may be granted by the Director of the Department of Technology and Innovation on a case-by-case basis.

11. Resources:

- Patch and Vulnerability Management Policy (City Eweb)
- Change Management Policy/Standard (City Eweb)
- Firewall Change Management Guidelines (Internal Wiki)
- NIST SP 800-41 - Guidelines for Firewalls and Firewall Policy (Relevant Sections: 2.1.1, 2.1.2, 4.1, 4.1.1, 4.1.3, 4.2, 4.5)
- NIST SP 800-53 - Security and Privacy Controls for Information Systems and Organizations (Relevant Sections: Control CM-7: Least Functionality, Control SI-4: Information System Monitoring, Control SC-7: Boundary Protection)

---

12. Revision History:

Version	Date	Description	Author	Approved By
1.0	12-19-2024	Initial Standard Draft	Anthony Ballo	DTI Security
1.1	1-3-2025	Draft Revisions	Anthony Ballo	DTI Security