



# State of Nevada

## Information Security Committee

### Banned Technology List

| Document ID | Title                  | Revision | Effective Date | Page   |
|-------------|------------------------|----------|----------------|--------|
| S.6.02.07.A | Banned Technology List | C        | 11/02/2023     | 1 of 2 |

#### 1.0 PURPOSE

This document contains the current list of technologies, including hardware, software, vendors, and services, that are banned from use in the State of Nevada due to security concerns.

#### 2.0 SCOPE

This Banned Technology list applies to all state agencies and authorized users meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

#### 3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval by the State Information Security Committee (SISC).

#### 4.0 RESPONSIBILITIES

The agency head and appointed Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this list and its associated standard.

#### 5.0 RELATED DOCUMENTS

State Information Security Program Policy, 100  
State Security Standard S.6.02.07 – Technology Bans

#### 6.0 BANNED TECHNOLOGY LIST

| Item  | Category          | Date Added |
|---|-------------------|------------|
| Alibaba products, including but not limited to AliPay * | Services          | 01/26/2023 |
| China Mobile International USA Inc. *                   | Services          | 01/26/2023 |
| China Telecom (Americas) Corp. *                        | Services          | 01/26/2023 |
| China Unicom (Americas) Operations Limited *            | Services          | 01/26/2023 |
| Dahua Technology Company *                              | Hardware/Vendor   | 01/26/2023 |
| Grammarly free public version                           | Software/Services | 11/02/2023 |
| Hangzhou Hikvision Digital Technology Company *         | Hardware/Vendor   | 01/26/2023 |
| Huawei Technologies *                                   | Hardware/Vendor   | 01/26/2023 |
| Hytera Communications Corporation *                     | Hardware/Vendor   | 01/26/2023 |



# State of Nevada

## Information Security Committee

### Banned Technology List

| Document ID | Title                  | Revision | Effective Date | Page   |
|-------------|------------------------|----------|----------------|--------|
| S.6.02.07.A | Banned Technology List | C        | 11/02/2023     | 2 of 2 |

|  |                   |            |
|--|-------------------|------------|
| Kaspersky *  | Software/Services | 01/26/2023 |
| Pacific Network Corp/ComNet (USA) LLC *  | Services          | 01/26/2023 |
| Tencent Holdings, including but not limited to Tencent QQ, QQ Wallet, and WeChat * | Software/Services | 01/26/2023 |
| TikTok   | Services          | 01/26/2023 |
| ZTE Corporation *  | Hardware/Vendor   | 01/26/2023 |

\* Item added due to Federal ban

#### 7.0 DEFINITIONS

#### 8.0 RESOURCES

Center for Internet Security (CIS), CIS Controls v7.1 Guide

FCC List of Equipment and Services Covered By Section 2 of The Secure Networks Act

#### 9.0 EXCEPTIONS

Requests for exception to the requirements of this list must be documented, provided to the OIS, and approved by the State CISO.

#### Approved By

| Title   | Signature             | Approval Date |
|---|-----------------------|---------------|
| State Information Security Committee            | Approved by Committee | 03/30/2023    |
| State Chief Information Security Officer (CISO) | Signature on file     | 11/02/2023    |
| State Chief Information Officer (CIO)           | Signature on file     | 11/02/2023    |

#### Document History

| Revision | Effective Date | Change  |
|----------|----------------|---|
| A        | 01/26/2023     | Initial release                               |
| B        | 03/30/2023     | Revised to remove potentially offensive terms |
| C        | 11/02/2023     | Specify version of Grammarly                  |