

Arizona Department Of Administration	Agency STANDARD A800-04-S01 Rev. 1.0	TITLE: <u>Configuration Change Control</u> Effective: November 09, 2009
---	---	--

1. AUTHORITY

- 1.1. The authority for this Standard is the Arizona Revised Statute 41-703 and the ADOA Policy A800 – Information Security.

2. PURPOSE

- 2.1. The purpose of this Standard is to establish the responsibilities and restrictions for performing configuration changes on any ADOA Critical Information System.

3. SCOPE

- 3.1. This Standard applies to all ADOA employees, contractors and other entities using ADOA Information Resources and Information Systems.
- 3.2. The ADOA Director, in conjunction with the ADOA Chief Information Officer (CIO) and the ADOA Information Security (AIS) Manager, is responsible for ensuring the effective implementation of ADOA Information Security Policy and Standards which reference the Statewide Information Technology Policies and Standards.

4. DEFINITIONS AND ABBREVIATIONS

- 4.1. **ADOA** – Arizona Department of Administration.
- 4.2. **AIS** - ADOA Information Security.
- 4.3. **AIS Manager** – ADOA Information Security Manager
- 4.4. **Business Hours** – the period of Monday through Friday and during the hours from 6 AM to 5 PM.
- 4.5. **CAB** – Change Advisory Board, allows or delays Requests for Change after assessing impact.
- 4.6. **Change** – is a modification to an ADOA Information Resource or Information System. All changes are required to be fully documented and undergo a formal approval process.
- 4.6.1. **Emergency Change** – are changes that **require immediate implementation** to maintain the integrity, availability, confidentiality and/or service levels of an ADOA Information Resource or Information System. An **Emergency Change** is initiated with an **Emergency Request for Change (RFC)**.
- 4.6.2. **Normal Change** – are planned changes that **do not require immediate implementation**, to maintain the integrity, availability, confidentiality and/or service levels of an ADOA Information

Resource or Information System. A **Normal Change** is initiated with a **Normal Request for Change (RFC)**.

4.6.3. Standard Change- are changes that pose low risk to the integrity, availability, confidentiality and/or service levels of an ADOA Information Resource or Information System. A **Standard Change** is initiated with a **Standard Request for Change (RFC)**.

- 4.7. Critical Information System** - An Information Resource or Information System that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. This includes applications that require special attention to security due to the risk and magnitude of harm resulting from the loss of availability, misuse, or unauthorized access to or modification of the information in the application.
- 4.8. Information Resource** - any computing device, peripheral, software, local and wide area network (LAN and WAN), communications equipment (including Fax machines and telephones), communications software (including the Internet, Intranet, and bulletin board access software), Virtual Private Network (VPN) or remote access capabilities and data distribution, electronic data or related consumable (e.g. paper, disk space, central processor time, network bandwidth) information and data owned or controlled by the ADOA.
- 4.9. Information System** - a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- 4.10. Information System Owner** – Person(s) responsible for the overall operation and maintenance of an ADOA Information Resource or Information System.
- 4.11. Maintenance Window** – is a defined and documented date and time before or after normal business hours, when the maintenance of ADOA Information Systems or Information Resources maybe performed.
- 4.12. RFC** – Request for Change.

5. STANDARD

- 5.1. There will be no changes to Critical ADOA Information Systems or to systems that affect Critical ADOA Information Systems during business hours and non-scheduled Maintenance Windows, unless by a properly approved Emergency Request for Change per 5.2.3 below.**
- 5.2.** Changes to any ADOA Critical Information System or to systems that affect Critical Information System are performed in accordance with the following:

5.2.1. Standard Request for Change

- 5.2.1.1. Standard RFC is initiated and tracked in the ADOA Remedy Change and Incident Tracking System.
- 5.2.1.2. Standard RFC is analyzed for risk, impact, and timing by approving Manager, who then approves or rejects the request.
- 5.2.1.3. If approved, the Standard RFC is planned, scheduled, and implemented by technician. If Standard RFC is rejected, requester is notified of reason.
- 5.2.1.4. Standard RFC is completed.

5.2.2. Normal Request for Change

- 5.2.2.1. Normal RFC initiated and recorded via the ADOA Remedy Change and Incident Tracking System.
- 5.2.2.2. Normal RFC is analyzed for risk, impact, and timing by approving Manager, who then approves or rejects the request.
- 5.2.2.3. Normal RFC moves to planned and scheduled if approved by Manager.
- 5.2.2.4. Normal RFC submitted to CAB.
- 5.2.2.5. CAB allows, delays or rejects the Normal RFC after analysis during weekly CAB meeting.
 - 5.2.2.5.1. Allowed Normal RFC begins implementation.
 - 5.2.2.5.2. Delayed Normal RFC returned to requester for further analysis, re-scheduling, more detail, etc and re-submitted to CAB.
 - 5.2.2.5.3. Rejected Normal RFC returned to requester for further analysis, re-scheduling, more detail, etc and re-submitted to CAB. Change implemented.
- 5.2.2.6. Normal RFC is completed.

5.2.3. Emergency Request for Change

5.2.3.1. The following, steps are required in the event of an Emergency Change:

- 5.2.3.1.1. Emergency RFC initiated and recorded via the ADOA Remedy Change and Incident Tracking System.
- 5.2.3.1.2. Emergency RFC is analyzed for risk, impact and timing by ADOA CIO, Deputy CIO or their

authorized representative, who then approves or rejects the emergency RFC.

- 5.2.3.1.3. Emergency RFC moves to planned and scheduled if approved by ADOA CIO, Deputy CIO or their authorized representative.
- 5.2.3.1.4. Emergency RFC requester must communicate with supporting Information System Owner(s) and other key stakeholders.
- 5.2.3.1.5. ADOA Help Desk must notify impacted ADOA customers and key stakeholders of the Emergency RFC.
- 5.2.3.1.6. Emergency RFC begins implementation.
- 5.2.3.1.7. Emergency RFC is completed.
- 5.2.3.1.8. CAB reviews completed Emergency RFC during weekly meetings to assess need for further documentation and to discuss root cause analysis.

6. STANDARD NON-COMPLIANCE

- 6.1. **All departments owning ADOA Information Resources and/or Information System are responsible for understanding and adhering to this Standard.**
- 6.2. **For non-compliance with this Standard, all ADOA employees shall be subject to Human Resource progressive discipline up to and including dismissal, with the exception that management may choose to take appropriate action commensurate with the seriousness of the offense. In addition, any non-compliance with this Standard that may constitute a violation of State or Federal criminal statute may be referred to a law enforcement agency for appropriate action.**
- 6.3. **Contractors and other authorized users will be held to contractual agreements or Service Level Agreements. In addition, any non-compliance with this Standard that may constitute a violation of State or Federal criminal statute may be referred to a law enforcement agency for appropriate action.**

7. REFERENCES

- 7.1. Statewide Policy – P800, IT Security
- 7.2. Statewide Standard – S815, Configuration Management
- 7.3. ADOA Policy A800 – Information Security

8. ATTACHMENTS

8.1. None