



# Information Systems Acquisition, Development, & Maintenance Policy

## Table of Contents

<b>1. Purpose</b>	<b>4</b>
<b>2. Scope</b>	<b>4</b>
<b>3. Target Audience</b>	<b>4</b>
<b>4. Roles &amp; Responsibilities</b>	<b>4</b>
<b>5. Compliance</b>	<b>5</b>
5.1 Compliance	5
5.2 Enforcement & Management	6
5.3 Monitoring & Review of Policy	6
5.4 Policy Approval	6
5.5 Exceptions	6
5.6 Document Location	6
<b>6. Policy</b>	<b>6</b>
6.1 Maintenance	6
6.2 Capital Planning	7
6.3 Secure Development Lifecycle	7
6.4 Information Security in Project Management	7
<b>7. Acquisition Security Requirements</b>	<b>7</b>
7.1 Security Requirements Identification	7
7.2 Third-Party Systems & Solutions	8
7.3 Evaluation, Procurement, & Implementation	8
7.3.1 Third-Party Evaluation Selection	8
7.3.2 Contractual Agreements & their Assurance	8
7.3.3 Development, Testing & Deployment	9
<b>8. Secure Application Development &amp; Maintenance</b>	<b>9</b>
8.1 Application Development & Deployment	9
8.1.1 Application Development	9
8.1.2 Change Management	10
8.2 Segregation of Duties, Controlling Application Code & Configurations	10
8.2.1 Development Environment	10
8.2.2 Production Environment	11
8.2.3 Migration	11
8.3 Quality Assurance (QA)	11
8.3.1 Secure QA	11
8.3.2 Controlled, Dedicated Test Environment	11
8.3.3 Test Data	11
8.3.4 Capacity Planning	12
8.4 Production Support	12

8.4.1 Exception, Error, & Outage Handling	12
8.5 Maintenance & Decommission	12
8.5.1 Security & Vendor Management	12
8.5.2 Licenses	13
8.5.3 Customer Support	13
8.5.4 Upgrades, Patching, Maintenance & Decommission	13
<b>9. Management of Public Key Infrastructure (PKI)</b>	<b>14</b>
9.1 Management Responsibility Delegation	15
9.2 Access to Cryptographic Keys	15
9.3 Storage of Cryptographic Keys	15
9.4 Generation of Strong Keys	15
9.5 Secure Key Distribution	15
9.6 Periodic Key Changes	15
9.7 Destruction of Old Keys	15
9.8 Prevention of Unauthorized Key Substitution	15
9.9 Replacement of Known or Suspected Compromised Keys	16
9.10 Revocation of Old or Invalid Keys	16
9.11 Key Custodian Responsibilities	16
<b>10. Securing Hardware</b>	<b>16</b>
10.1 Purchasing, Installing, Issuing Hardware	16
10.1 Cabling and Power Supplies	16
10.2 Consumables	17
10.3 Additional Hardware Maintenance Policies	17
<b>11. References</b>	<b>17</b>
<b>12. Definitions and Acronyms</b>	<b>17</b>
<b>13. Revision History</b>	<b>18</b>
<b>14. Approvals</b>	<b>18</b>