NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
CA-1	Management	CA-01	Security Assessment Policy & Procedures	CA-1			8-200 8-201 8-202 8-610						5.1.1, 5.1.2, 6.1.1, 18.2.1, 6.1.1, 12.1.1, 18.1.1 & 18.2.2										Management	Basic
CA-2	Management	CA-02	Security Assessments	CA-2	3.12.1 3.12.2 3.12.3 3.12.4		8-610	CC4.1	CC4.1				14.2.8, 14.2.9, 16.1.3, 18.2.1, 18.2.2 & 18.2.3	ID.RA-1, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5 & RS.CO-3			17.03(2)(h)	622(2)(B)(i)-(iv)			Technical Users	Basic
CA-2 (1)	Management	CA-02(a)	Security Assessments | Independent Assessors	CA-2 (1)																		Management	Enhanced
CA-2 (2)	Management	CA-02(b)	Security Assessments | Specialized Assessments	CA-2 (2)																		Management	Enhanced
CA-2 (3)	Management	CA-02(c)	Security Assessments | External Organizations	CA-2 (3)																		Management	Enhanced
CA-3	Management	CA-03	Information System Connections	CA-3			8-610						15.1.2, 13.1.2, 13.2.1 & 13.2.2	& DE.AE-1	12.1 12.2 12.3 12.4 12.5 12.6 12.7 12.8 12.9 12.10							All Users	Basic
CA-3 (3)	Management	CA-03(a)	Information System Connections | Unclassified Non-National Security System Connections	CA-3 (3)																		Management	Enhanced
CA-3 (5)	Management	CA-03(b)	Information System Connections | Restrictions on External System Connections	CA-3 (5)								.3.5										Technical Users	Basic
N/A	Management	CA-03(c)	Information System Connections | Demilitarized Zones (DMZs)									1.3.1, .3.4										Technical Users	Basic
N/A	Management	CA-03(d)	Information System Connections | Guest Networks									1.2.3										All Users	Basic
CA-4	Management	CA-04	Security Verification																			Technical Users	Basic
CA-5	Management	CA-05	Plan of Action and Milestones (POA&M)	CA-5	3.12.1 3.12.2 3.12.3 3.12.4		8-610															Technical Users	Basic
CA-6	Management	CA-06	Security Authorization	CA-6			8-202 8-610 8-614						14.2.9									Management	Basic
CA-7	Management	CA-07	Continuous Monitoring	CA-7	3.12.1 3.12.2 3.12.3 3.12.4		8-						18.2.1, 12.6.1, 16.1.3, 18.2.2 & 18.2.3	ID.RA-1, PR.IP-7, PR.IP-8, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1, RS.CO-3 & RS.MI-3				622(2)(B)(iii)				Management	Basic
CA-7 (1)	Management	CA-07(a)	Continuous Monitoring | Independent Assessment	CA-7 (1)																		Management	Enhanced
CA-8	Management	CA-08	Penetration Testing	CA-8			8-610 8-614				500.05	11.3-11.3.3		ID.RA-1	20.1 20.2 20.3 20.4 20.5 20.6 20.7 20.8							Management	Enhanced
CA-8 (1)	Management	CA-08(a)	Penetration Testing | Independent Penetration Agent or Team	CA-8 (1)											20.2							Management	Enhanced
CA-8 (2)	Management	CA-08(b)	Penetration Testing | Red Team Exercises																			Management	Enhanced
CA-9	Management	CA-09	Internal System Connections	CA-9			8-610 8-700															Technical Users	Enhanced
PL-1	Management	PL-01	Security Planning Policy & Procedures	PL-1			8-101 8-311						5.1.1, 5.1.2, 6.1.1, 12.1.1, 18.1.1 & 18.2.2	ID.AM-3								Management	Basic

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
PL-2	Management	PL-02	System Security Plan (SSP)	PL-2	3.12.1 3.12.2 3.12.3 3.12.4		8-311 8-610	CC2.4	CC2.4				6.1.2	PR.IP-7 & DE.DP-5								Technical Users	Basic
PL-2 (3)	Management	PL-02(a)	System Security Plan (SSP) | Plan / Coordinate with Other Organizational Entities	PL-2 (3)																		Technical Users	Basic
N/A	Management	PL-02(b)	System Security Plan (SSP) | Adequate Security for Covered Defense Information (CDI)														17.03(2)(b)(i)					Technical Users	Basic
PL-3	Management	PL-03	System Security Plan Update																			Technical Users	Basic
PL-4	Management	PL-04	Rules of Behavior	PL-4			8-103	CC1.4	CC1.4			4.2, 12.3, 12.3.1, 12.3.2, 12.3.5-.6, 12.3.10 &12.4	13.2.4, 15.1.2, 8.1.3, 7.2.1, 13.2.1, 6.2.1, 6.2.2 & 16.1.3			164.310(b)	17.03(2)(b)(2)					All Users	Basic
PL-4 (1)	Management	PL-04(a)	Rules of Behavior | Social Media & Social Networking Restrictions	PL-4 (1)				CC1.4	CC1.4													All Users	Basic
PL-5	Management	PL-05	Privacy Impact Assessment (PIA)											ID.RA-4	13.1							Technical Users	Basic
PL-6	Management	PL-06	Security-Related Activity Planning [withdrawn - incorporated in PL-2]																			N/A	N/A
PL-7	Management	PL-07	Security Concept Of Operations				8-610						14.1.1									Management	Basic
PL-8	Management	PL-08	Security Architecture	PL-8									14.1.1	ID.								Management	Basic
PL-9	Management	PL-09	Central Management					CC1.1	CC1.1													Management	Basic
PM-1	Management	PM-01	Information Security Program Plan				8-100	CC7.2	CC7.2	8.2.1	500.02 500.03	12.1 & 12.	5.1.1, 6.1	SV-1 & ID.GV-2		164.308(a)(1)(i) & 164.316(a)-(b)	17.03(1), 17.04 & 17.03(2)(b)(2)			6801(b)(1)		Management	Basic
PM-2	Management	PM-02	Assigned Information Security Responsibilities				8-101	CC1.1	CC1.1	1.1.2		5-12	6.1	ID.AM-6 & ID.GV-2		164.308(a)(2)	17.03(2)(a)	622(2)(d)(A)(i)		Safeguards Rule		Management	Basic
PM-3	Management	PM-03	Information Security Resources																			Management	Basic
PM-4	Management	PM-04	Vulnerability Remediation Process				8-311							ID.RA-6			17.03(2)(j)	622(2)(d)(B)(iii)				Management	Basic
PM-5	Management	PM-05	Information System Inventory				8-311					3, 12.3.4 & 12.3.7	8.1.1 & 8.1.2	ID.AM-1 & ID.AM-2	1.1 1.2 1.3 1.4 1.5 1.6							Management	Basic
PM-6	Management	PM-06	Information Security Measures of Performance				8-311	CC1.1		8.2.7				ID.AM-2 & PR.IP-7		164.308(a)(8)	17.03(2)(j)	622(2)(d)(A)(vi) & 622(2)(d)(B)(iii)				Management	Basic
PM-7	Management	PM-07	Enterprise Architecture				8-103					2.2										Management	Basic
N/A	Management	PM-07(a)	Enterprise Architecture | Standardized Terminology																			Management	Basic
PM-8	Management	PM-08	Regulatory & Non-Regulatory Compliance				8-10		A1.3			12.1		ID.BE-2, ID.BE-4, ID.GV-3 & ID.RM-3		164.308(a)(8)				6801(b)(3)		Management	Basic
PM-9	Management	PM-09	Risk Management Strategy				3				500.09	12.2	18.2.1 & 17.1.1	ID.GV-4, ID.RA-3, ID.RA-4, ID.RA-6, ID.RM-1, ID.RM-2 & ID.RM-3		164.308(a)(1)(ii)(B)	17.03(2)(b)	622(2)(d)(A)(ii)		6801(b)(2)		Management	Basic
PM-10	Management	PM-10	Security Authorization Process				8-3						6.1.1									Management	Basic
PM-11	Management	PM-11	Business Process Definition				8-303							ID.AM-6, ID.BE-3, ID.GV-4, ID.RA-4 & ID.RM-3								Management	Basic
PM-12	Management	PM-12	Insider Threat Program											ID.RA-3								Management	Enhanced
PM-13	Management	PM-13	Information Security Workforce				8-103 8-307	CC1.2 CC2.3	CC1.2 CC2.3		500.14		7.2.2	PR.AT-1, PR.AT-2, PR.AT-4 & PR.AT-5								Management	Enhanced
PM-14	Management	PM-14	Testing, Training, and Monitoring				8-302			8.2.7			7.2.2	PR.IP-10, DE.DP-1, DE.DP-2, DE.DP-3 & DE.DP-5								Management	Basic
PM-15	Management	PM-15	Contacts with Security Groups and Associations				8-101				500.10	5.1.2 & 6.1		ID.RA-2 & RS.CO-5		164.308(A)(5)(ii) & (ii)(A)						Management	Basic
PM-16	Management	PM-16	Threat Awareness Program				8-103	CC3.1	CC3.1			12.6	6.1.4	ID.RA-2, ID.RA-3 & ID.RA-5	4.4							Management	Enhanced
RA-1	Management	RA-01	Risk Assessment Policy & Procedures	RA-1			8-610				500.09		5.1.1, 5.1.2, 6.1.1, 12.1.1, 18.1.1 & 18.2.2				17.03(2)(b)					Management	Basic
RA-2	Management	RA-02	Security Categorization	RA-2			8-402	CC2.1	CC2.1			9.6.1	8.2.1 & 14.1.1	ID.AM-5, ID.RA-4 & ID.RA-5								Management	Basic
RA-3	Management	RA-03	Risk Assessment	RA-3	3.11.1		8-402			1.2.4	500.09	12.2	12.6.1 & 17.1.1	ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, PR.IP-12, DE.AE-4 & RS.MI-3		164.308(a)(1)(ii)(A) & (B)	17.03(2)(b)	622(2)(A)(ii)		Safeguards Rule		Management	Basic

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
N/A	Management	RA-03(a)	Risk Assessment | Risk Ranking												4.8							Technical Users	Basic
RA-4	Management	RA-04	Risk Assessment Update									6.1					17.03(2)(i) & 17.03(2)(b)(3)	622(2)(A)(iv)		Safeguards Rule		Management	Basic
RA-5	Management	RA-05	Vulnerability Scanning	RA-5	3.11.2 3.11.3	15	8-614				500.05	11.2	12.6.1 & 18.2.3	ID.RA-1, PR.IP-12, DE.CM-8, DE.DP-4, DE.DP-5, RS.CO-3 & RS.MI-3	4.1 4.2 4.3 4.6 4.7 15.2			622(2)(B)(iii) & 622(2)(d(A)(iii)				Management	Basic
RA-5 (1)	Management	RA-05(a)	Vulnerability Scanning | Update Tool Capability	RA-5 (1)							500.05											Technical Users	Enhanced
RA-5 (2)	Management	RA-05(b)	Vulnerability Scanning | Update by Frequency / Prior to New Scan / When Identified	RA-5 (2)																		Technical Users	Enhanced
RA-5 (3)	Management	RA-05(c)	Vulnerability Scanning | Bredth / Depth of Coverage	RA-5 (3)																		Technical Users	Basic
RA-5 (5)	Management	RA-05(d)	Vulnerability Scanning | Privileged Access	RA-5 (5)	3.11.2																	Technical Users	Enhanced
RA-5 (6)	Management	RA-05(e)	Vulnerability Scanning | Automated Trend Analysis	RA-5 (6)																		Technical Users	Basic
RA-5 (8)	Management	RA-05(f)	Vulnerability Scanning | Review Historic Audit Logs	RA-5 (8)																		Technical Users	Basic
N/A	Management	RA-05(g)	Vulnerability Scanning | External Vulnerability Assessment Scans for PCI DSS Compliance									11.2, 11.2.2 & 11.2.3										Technical Users	Enhanced
N/A	Management	RA-05(h)	Vulnerability Scanning | Internal Vulnerability Assessment Scans for PCI DSS Compliance									11.2, 11.2.2 & 11.2.3										Technical Users	Enhanced
RA-6	Management	RA-06	Technical Surveillance Countermeasures Survey																			Management	Enhanced
SA-1	Management	SA-01	System & Services Acquisition Policy & Procedures	SA-1									5.1.1, 12.1.1, 14. & 18.2.2		18.1							Management	Basic
SA-2	Management	SA-02	Allocation of Resources	SA-2			8-100 8-200						12.1.3									Management	Basic
SA-3	Management	SA-03	System Develop Life Cycle (SDLC)	SA-3			8-311 8-610	CC7.1	CC7.1				6.1.1 & 14.1.1	PR.IP-2								Technical Users	Basic
SA-4	Management	SA-04	Acquisition Process	SA-4			8-302 8-613	C1.5 C1.7					14.2.9 & 14.2.7	PR.IP-2 & DE.CM-6	18.2 18.3 18.4 18.5 18.6 18.7 18.8 18.9							Technical Users	Basic
SA-4 (1)	Management	SA-04(a)	Acquisition Process | Functional Properties Of Security Controls	SA-4 (1)																		Technical Users	Enhanced
SA-4 (2)	Management	SA-04(b)	Acquisition Process | Design & Implementation of Security Controls	SA-4 (2)																		Technical Users	Enhanced
SA-4 (3)	Management	SA-04(c)	Acquisition Process | Development Methods																			Technical Users	Enhanced
SA-4 (6)	Management	SA-04(d)	Acquisition Process | Commercial Off-The-Shelf (COTS) Security Solutions																			Technical Users	Basic
SA-4 (8)	Management	SA-04(e)	Acquisition Process | Continuous Monitoring Plan	SA-4 (8)																		Technical Users	Enhanced
SA-4 (9)	Management	SA-04(f)	Acquisition Process | Functions / Ports / Protocols / Services in Use	SA-4 (9)																		Technical Users	Enhanced
SA-4 (10)	Management	SA-04(g)	Acquisition Process | Use of Approved PIV Products	SA-4 (10)																		Technical Users	Enhanced
SA-5	Management	SA-05	Information System Documentation	SA-5			8-202 8-320 8-610				500.08		12.1.1, 16.1.3 & 18.1.3	ID.RA-1								Technical Users	Basic
SA-5 (1)	Management	SA-05(a)	Information System Documentation | Functional Properties Of Security Controls																			Technical Users	Enhanced
SA-5 (2)	Management	SA-05(b)	Information System Documentation | External System Interfaces			3																Technical Users	Enhanced
SA-5 (3)	Management	SA-05(c)	Information System Documentation | High-Level Design																			Technical Users	Enhanced
SA-5 (4)	Management	SA-05(d)	Information System Documentation | Low-Level Design																			Technical Users	Enhanced
SA-5 (5)	Management	SA-05(e)	Information System Documentation | Source Code																			Technical Users	Enhanced
SA-6	Management	SA-06	Software Usage Restrictions [withdrawn - incorporated in CM-10 & SI-07]																			N/A	N/A
SA-7	Management	SA-07	User-Installed Software [withdrawn - incorporated in CM-11 & SI-07]																			N/A	N/A

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
SA-8	Management	SA-08	Secure Engineering Principles	SA-8	3.13.1 3.13.2	4	8-311	CC3.2	CC3.2		500.08	2.2	10.4.2 ,14.1.1 & 14.2.5	PR.IP-2	1.2, 5.9, 6.2, 6.3, 6.4, 6.5, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 8.6, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 11.4, 11.5, 11.6, 11.7, 13.4, 13.5, 16.5							Technical Users	Basic
SA-9	Management	SA-09	External Information Systems	SA-9		3, 4	8-700						6.1.1, 13.2.4, 15.1.2, 7.2.1, 15.2.1, 13.2.2 & 14.2.7	ID.AM-4, PR.AT-3 & DE.CM-6			17.03(2)(f)(1)	622(2)(d)(A)(v)				Technical Users	Basic
SA-9 (1)	Management	SA-09(a)	External Information System Services | Risk Assessments & Organizational Approvals	SA-9 (1)		3						2.4, 12.8- 12.8.4				164.308(a)(b)(1), 164.308(a)(4)(1) & 164.314(a)	17.03(2)(f)(2)	622(2)(d)(A)(v)		Safeguards Rule		Technical Users	Basic
SA-9 (2)	Management	SA-09(b)	External Information System Services | Identification Of Functions, Ports, Protocols & Services	SA-9 (2)		3																Technical Users	Basic
SA-9 (3)	Management	SA-09(c)	External Information System Services | Business Partner Contracts			3		C1.4	C1.4			2.6 & 1				164.308(b)(1), 164.314(a)(1)(i)-(ii), 164.314(a)(1)(ii)(A)-(B), 164.314(a)(2)(i)(A)-(D), 164.314(a)(2)(i)(A)-(D), 164.314(a)(2)(ii)(1)-(2)						Management	Basic
SA-9 (4)	Management	SA-09(d)	External Information System Services | Consistent Interests of Consumers and Providers	SA-9 (4)		3																Management	Enhanced
SA-9 (5)	Management	SA-09(e)	External Information System Services | Processing, Storage and Service Location	SA-9 (5)		3																Management	Enhanced
N/A	Management	SA-09(f)	External Information Systems | Group Health Plans													164.314(b)(1)-(2)						Management	Enhanced
SA-10	Management	SA-10	Developer Configuration Management	SA-10			8-613						12.1.2, 12.1.4, 15.2.2, 14.2.9, 9.4.5, 14.2.2 & 14.2.7	PR.IP-1, PR.IP-2 & PR.IP-3	18.2 18.3 18.4 18.5 18.6 18.7 18.8 18.9		17.03(2)(d)(B)(i)					Management	Basic
SA-10 (1)	Management	SA-10(a)	Developer Configuration Management | Software / Firmware Integrity Verification	SA-10 (1)																		Technical Users	Enhanced
SA-11	Management	SA-11	Developer Security Testing	SA-11								6.4 & 6.4.4	18.2.1, 14.2.9, 14.2.7 & 16.1.3	ID.RA-1 & PR.IP-2			17.03(2)(d)(B)(i)					Technical Users	Basic
SA-11 (1)	Management	SA-11(a)	Developer Security Testing | Static Code Analysis	SA-11 (1)								6.3, 6.3.1 & 6.3.2										Technical Users	Enhanced
SA-11 (2)	Management	SA-11(b)	Developer Security Testing | Threat Analysis & Flaw Remediation	SA-11 (2)								6.6										Technical Users	Basic
SA-11 (8)	Management	SA-11(c)	Developer Security Testing | Dynamic Code Analysis	SA-11 (8)																		Technical Users	Enhanced
SA-12	Management	SA-12	Supply Chain Protection								500.11		14.2.7	ID.BE-1 & PR.IP-2								Management	Basic
SA-12 (1)	Management	SA-12(a)	Supply Chain Protection | Acquisition Strategies, Tools & Methods																			Management	Enhanced
SA-12 (2)	Management	SA-12(b)	Supply Chain Protection | Supplier Reviews								500.11											Management	Enhanced
SA-12 (5)	Management	SA-12(c)	Supply Chain Protection | Liability of Harm																			Management	Enhanced
SA-12 (10)	Management	SA-12(d)	Supply Chain Protection | Validate as Genuine & Not Altered																			Technical Users	Enhanced
SA-12 (15)	Management	SA-12(e)	Supply Chain Protection | Processes to Address Weaknesses or Deficiencies																			Management	Enhanced
SA-13	Management	SA-13	Trustworthiness				8-302 8-311						14.2.7									Management	Enhanced
SA-14	Management	SA-14	Criticality Analysis					CC2.2	CC2.2		500.11			ID.AM-5, ID.BE-3, ID.BE-4, ID.BE-5, ID.RA-4 & ID.RM-3								Management	Enhanced
SA-15	Management	SA-15	Development Process, Standards, and Tools	SA-15								6.3, 6.5, 6.5.1-6.5.10	14.3.1 & 14.2.7	PR.IP-2								Technical Users	Basic
SA-15 (9)	Management	SA-15(a)	Development Process, Standards, and Tools | Use of Live Data									6.4 & 6.4.3					17.03(2)(d)(B)(i)					Technical Users	Basic
SA-16	Management	SA-16	Developer-Provided Training	SA-16									7.2.2									Management	Basic

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
SA-17	Management	SA-17	Developer Security Architecture and Design	SA-17										PR.IP-2								Technical Users	Basic
SA-18	Management	SA-18	Tamper Resistance and Detection				8-308															Technical Users	Enhanced
SA-18 (2)	Management	SA-18(a)	Tamper Resistance and Detection | Inspection of Information Systems, Components or Devices									9.1, 9.1.1, 9.9 & 9.9.1-9.9.3										Technical Users	Enhanced
SA-19	Management	SA-19	Component Authenticity				8-302															Management	Basic
SA-19 (1)	Management	SA-19(a)	Component Authenticity | Anti-Counterfeit Training																			Management	Enhanced
SA-19 (3)	Management	SA-19(b)	Component Authenticity | Component Disposal																			Technical Users	Basic
SA-20	Management	SA-20	Customized Development of Critical Components																			Technical Users	Enhanced
SA-21	Management	SA-21	Developer Screening										7.1.1									Management	Basic
SA-22	Management	SA-22	Unsupported System Components				8-302															Technical Users	Basic
SA-22 (1)	Management	SA-22(a)	Unsupported System Components | Alternate Sources for Continued Support																			Technical Users	Basic
AT-1	Operational	AT-01	Security Awareness & Training Policy & Procedures	AT-1			8-101				500.14		5.1.1, 5.1.2, 6.1.1, 12.1.1, 18.1.[illegible] 18.2.1									Management	Basic
AT-2	Operational	AT-02	Security Awareness	AT-2	3.2.1 3.2.2		8-101				500.14	12.6	7.2.2 & 12.2.1	[illegible]AT-1	17.3	164.308(a)(5)(i) & 164.308(a)(5)(ii)(A)	17.04(8) & 17.03(2)(b)(1)					Management	Basic
AT-2 (1)	Operational	AT-02(a)	Security Awareness | Practical Exercises												17.4							Management	Enhanced
AT-2 (2)	Operational	AT-02(b)	Security Awareness | Insider Threat	AT-2 (2)	3.2.3																	Management	Enhanced
AT-3	Operational	AT-03	Security Training	AT-3	3.2.1 3.2.2		8-101 8-103 8-104				500.10 500.14	12.6	[illegible]2.2.1	PR.AT-2, PR.AT-4 & PR.AT-5	17.1 17.2		17.04(8)	622(2)(d)(A)(iv				Management	Basic
N/A	Operational	AT-03(a)	Security Training | Awareness Training for Sensitive Information									[illegible]3.[illegible]9.4, 9.10, 12.6, 12.8.3, 12.10										Management	Enhanced
N/A	Operational	AT-03(b)	Security Training | Vendor Security Training																			Technical Users	Enhanced
AT-4	Operational	AT-04	Security Training Records	AT-4			8-103 8-104					12.6.2										Management	Basic
AT-5	Operational	AT-05	Security Industry Alerts & Notification Process									6.2 & 12.4				164.308(A)(5)(ii) & (ii)(A)						Technical Users	Basic
CP-1	Operational	CP-01	Contingency Planning Policy & Procedures	CP-1			8-603	A1.3	A[illegible]				5.1.1, 5.1.2, 6.1.1, 12.1.1, 17.1.2, 17.1.2, 18.1.1 & 18.2.2			164.308(a)(7)(i) / 164.308(a)(7)(ii)							Management	Basic
CP-2	Operational	CP-02	Contingency Plan	CP-2			[illegible]	[illegible].3	A1.3				6.1.1, 11.1.3, 12.1.3, 17.1.2, 17.1.1 & 17.1.3	ID.AM-5, ID.AM-6, ID.BE-1, ID.BE-5, PR.DS-4, PR.IP-7, PR.IP-9, DE.AE-4, RS.AN-2, RS.AN-4, RS.CO-1, RS.CO-3, RS.CO-4, RS.IM-1, RS.IM-2, RS.RP-1, RC.IM-1, RC.IM-2 & RC.CO-3		164.308(a)(7)(ii)(C) & 164.312(a)(2)(ii)						Management	Basic
CP-2 (1)	Operational	CP-02(a)	Contingency Plan | Coordinate with Related Plans	CP-2 (1)																		Management	Basic
CP-2 (2)	Operational	CP-02(b)	Contingency Plan | Capacity Planning	CP-2 (2)																		Management	Enhanced
CP-2 (3)	Operational	CP-02(c)	Contingency Plan | Resume Essential Missions / Business Functions	CP-2 (3)																		Management	Basic
CP-2 (8)	Operational	CP-02(d)	Contingency Plan | Identify Critical Assets	CP-2 (8)																		Management	Basic
CP-3	Operational	CP-03	Contingency Training	CP-3			8-615						7.2.2	RS.CO-1								Management	Basic
CP-4	Operational	CP-04	Contingency Plan Testing	CP-4			8-615						17.1.2 & 17.1.3			164.308(a)(7)(ii)(D)						Management	Basic
CP-4 (1)	Operational	CP-04(a)	Contingency Plan Testing | Coordinate with Related Plans	CP-4 (1)																		Management	Basic
CP-5	Operational	CP-05	Contingency Plan Update											PR.IP-4 & PR.IP-10		164.308(a)(7)(ii)(e)						Management	Basic
CP-6	Operational	CP-06	Alternate Storage Site	CP-6			8-603						11.1.4 & 17.1.2	PR.IP-4		164.310(a)(2)(i)						Management	Enhanced
CP-6 (1)	Operational	CP-06(a)	Alternate Storage Site | Separation from Primary Site	CP-6 (1)																		Management	Enhanced
CP-6 (3)	Operational	CP-06(b)	Alternate Storage Site | Accessibility	CP-6 (3)																		Management	Enhanced
CP-7	Operational	CP-07	Alternate Processing Site	CP-7			8-603						11.1.4 & 17.1.2									Management	Enhanced
CP-7 (1)	Operational	CP-07(a)	Alternate Processing Site | Separation from Primary Site	CP-7 (1)																		Management	Enhanced
CP-7 (2)	Operational	CP-07(b)	Alternate Processing Site | Accessibility	CP-7 (2)																		Management	Enhanced
CP-7 (3)	Operational	CP-07(c)	Alternate Processing Site | Priority of Service	CP-7 (3)																		Management	Enhanced

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
CP-8	Operational	CP-08	Telecommunications Services	CP-8			8-615						11.2.2 & 17.1.2	ID.BE-4 & PR.PT-4								Management	Basic
CP-8 (1)	Operational	CP-08(a)	Telecommunications Services | Priority-of-Service Provisions	CP-8 (1)																		Management	Enhanced
CP-8 (2)	Operational	CP-08(b)	Telecommunications Services | Single Points of Failure	CP-8 (2)																		Management	Enhanced
CP-9	Operational	CP-09	Information System Backup	CP-9	3.8.9		8-603 8-612						12.3.1, 17.1.2 & 18.1.3	PR.IP-4	10.1 10.3	164.308(a)(7)(ii)(A						Technical Users	Basic
CP-9 (1)	Operational	CP-09(a)	Information System Backup | Testing for Reliability & Integrity	CP-9 (1)											10.2							Technical Users	Basic
CP-9 (3)	Operational	CP-09(b)	Information System Backup | Separate Storage for Critical Information	CP-9 (3)																		Technical Users	Enhanced
CP-10	Operational	CP-10	Information System Recovery & Reconstitution	CP-10			8-613						17.1.2	RS.RP-1 & RC.RP-1	10.4	164.308(a)(7)(ii)(B)						Technical Users	Basic
CP-10 (2)	Operational	CP-10(a)	Information System Recovery & Reconstitution | Transaction Recovery	CP-10 (2)											10.4							Technical Users	Enhanced
CP-10 (5)	Operational	CP-10(b)	Information System Recovery & Reconstitution | Failover Capability												10.4							Technical Users	Enhanced
CP-10 (6)	Operational	CP-10(c)	Information System Recovery & Reconstitution | Backup & Restoration Hardware Protection												10.4							Technical Users	Enhanced
N/A	Operational	CP-10(d)	Information System Recovery & Reconstitution | Electronic Discovery (eDiscovery)												10.4							Technical Users	Enhanced
N/A	Operational	CP-10(e)	Information System Recovery & Reconstitution | Information System Imaging												10.4							Technical Users	Enhanced
CP-11	Operational	CP-11	Alternate Communications Protocols				8-601 8-603 8-615						17.	ID.BE-5								Technical Users	Enhanced
CP-12	Operational	CP-12	Safe Mode				8-615															Technical Users	Enhanced
CP-13	Operational	CP-13	Alternative Security Mechanisms				8-605 8-607 8-610						17.1.2									Technical Users	Enhanced
IR-1	Operational	IR-01	Incident Response Policy & Procedures	IR-1			8-101 8-103			1.2			5.1.1, 5.1.2, 6.1.1, 12.1.1, 16.1.2, 16.1.1, 18.1.1 & 18.2.2		19.1	164.308(a)(6)(i)						Management	Basic
IR-2	Operational	IR-02	Incident Response Training	IR-2	3.6.1 3.6.2		8-103 8-104						7.2.2 & 12.2.1		19.7							Management	Basic
IR-3	Operational	IR-03	Incident Response Testing	IR-3	3.6.3		8-104							PR.IP-10 & RS.CO-1	19.7							Management	Basic
IR-3 (2)	Operational	IR-03(a)	Incident Response Testing | Coordination with Related Plans	IR-3 (2)						1.2.7					19.7							Management	Basic
IR-4	Operational	IR-04	Incident Handling	IR-4	3.6.1 3.6.2		1-303 4-218			1.2.7	500.16	12.5.3	6.1.3, 16.1.1, 16.1.4, 16.1.6 & 16.1.7	DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.CO-3, RS.CO-4, RS.IM-1, RS.IM-2, RS.MI-1, RS.MI-2, RS.RP-1, RC.RP-1, RC.IM-1, RC.IM-2 & RC.CO-3	19.1							Management	Basic
IR-4 (1)	Operational	IR-04(a)	Incident Handling | Automated Incident Handling Processes	IR-4 (1)																		Management	Enhanced
N/A	Operational	IR-04(b)	Incident Handling | Identity Theft Protection Program (ITPP)																X			Management	Enhanced
IR-5	Operational	IR-05	Incident Monitoring	IR-5	3.6.1 3.6.2		1-303 4-218			1.2.7		12.5.2		DE.AE-3, DE.AE-5, RS.AN-1 & RS.AN-4								Management	Basic
IR-6	Operational	IR-06	Incident Reporting	IR-6	3.6.1 3.6.2		1-303 4-218	CC2.5	CC2.5	1.2.7	500.16 500.17	12.8.3	6.1.3 & 16.1.2	RS.CO-2		164.308(a)(6)(ii)	17.03(2)(j)	604(1)-(5)				All Users	Basic
IR-6 (1)	Operational	IR-06(a)	Incident Reporting | Automated Reporting	IR-6 (1)																		Management	Enhanced
IR-6 (2)	Operational	IR-06(b)	Incident Reporting | Cyber Incident Reporting for Covered Defense Information (CDI)																			Management	Enhanced
IR-7	Operational	IR-07	Incident Response Assistance	IR-7	3.6.1 3.6.2					1.2.7	500.17		6.1.3		19.5							Management	Basic
IR-7 (1)	Operational	IR-07(a)	Incident Response Assistance | Automation Support of Availability of Information / Support	IR-7 (1)									6.1.3									Management	Enhanced

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
IR-7 (2)	Operational	IR-07(b)	Incident Response Assistance | Coordination With External Providers	IR-7 (2)							500.16			RS.CO-1, RS.CO-4, RC.CO-1, RS.CO-2 & RS.CO-3								Management	Enhanced
IR-8	Operational	IR-08	Incident Response Plan (IRP)	IR-8			8-103 1-302	CC6.2	CC6.2	1.2.8	500.16	12.8.3, 12.10, 12.10.1-12.10.6	12.2.1	PR.IP-7, PR.IP-9, DE.AE-3, DE.AE-5, RS.AN-4, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.IM-1, RS.IM-2, RS.RP-1, RC.RP-1, RC.IM-1 & RC.IM-2	19.1 19.4 19.5 19.6	164.308(a)(6)(ii)		622(2)(d)(B)(iii)				Management	Basic
IR-9	Operational	IR-09	Information Spillage Response	IR-9			8-103															Management	Basic
IR-9 (1)	Operational	IR-09(a)	Information Spillage Response | Responsible Personnel	IR-9 (1)																		Management	Enhanced
IR-9 (2)	Operational	IR-09(b)	Information Spillage Response | Training	IR-9 (2)																		Management	Enhanced
IR-9 (3)	Operational	IR-09(c)	Information Spillage Response | Post-Spill Operations	IR-9 (3)																		Management	Enhanced
IR-9 (4)	Operational	IR-09(d)	Information Spillage Response | Exposure to Unauthorized Personnel	IR-9 (4)																		Management	Enhanced
IR-10	Operational	IR-10	Integrated Information Security Analysis Team								500.16		.6		19.2 19.3							Management	Basic
MP-1	Operational	MP-01	Media Protection Policy & Procedures	MP-1			8-306 8-309	C1.1	C1.1				5.1.1, 5. 12.1.1, 8.3. .1.1, 11.2.9, 10.1.1, 18.1.1, 18.1.3 & 18.2.2			164.308(a)(4)(ii)(B)	17.03(2)(c)						Management	Basic
MP-2	Operational	MP-02	Media Access	MP-2	3.8.1 3.8.2 3.8.3		8-310	C1.2	C1.2				8.1.2, 8.2.3, 8.3.1 & 11.2.9	PR.PT-2		164.308(a)(4)(ii)(C)						Technical Users	Basic
MP-2 (1)	Operational	MP-02(a)	Media Access | Automated Restricted Access																			Technical Users	Basic
N/A	Operational	MP-02(b)	Media Access | Disclosure of Information																			All Users	Basic
MP-3	Operational	MP-03	Media Marking	MP-3	3.8.4		8-306 8-310			.3			8.2.2 & 8.2.3									All Users	Basic
MP-4	Operational	MP-04	Media Storage	MP-4	3.8.1 3.8.2 3.8.3		8-308					9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.7 & 9.9	8.2.3, 8.3.1, 11.2.9 & 18.1.3	PR.PT-2		164.310(d)(2)(iv)	17.03(2)(c)	622(2)(d)(C)(i) & 620				All Users	Basic
MP-4 (1)	Operational	MP-04(a)	Media Storage | Cryptographic Protection (Encrypting Data At Rest)								500.15	3.4, 3.4.1 & 9.8.2			13.2							All Users	Enhanced
N/A	Operational	MP-04(b)	Media Storage | Sensitive Data Inventories									9.7.1										Management	Enhanced
MP-5	Operational	MP-05	Media Transportation	MP-5	3.8.5			CC5.7	CC5.7	8.2.6		9.6, 9.6.2, 9.6.3 & 9.7	8.2.3, 8.3.1, 8.3.3, 11.2.5 & 11.2.6	PR.PT-2		164.310(d)(1)	17.03(2)(c)	620				All Users	Basic
MP-5 (3)	Operational	MP-05(a)	Media Transportation | Custodians																			All Users	Basic
MP-5 (4)	Operational	MP-05(b)	Media Transportation | Cryptographic Protection (Encrypting Data In Storage Media)	MP-5 (4)	3.8.6						500.15											All Users	Basic
N/A	Operational	MP-05(c)	Media Transportation | Ad-Hoc Transfers							8.2.6												All Users	Basic
MP-6	Operational	MP-06	Media Sanitization	MP-6	3.8.1 3.8.2 3.8.3	7	8-301 8-608	C1.8	C1.8			9.8, 9.8.1 & 9.8.2	8.2.3, 8.3.1, 8.3.2, 11.2.5, 11.2.6 & 11.2.7	PR.DS-3 & PR.IP-6		164.310(d)(2)(i)		622(2)(d)(C)(i) & 622(2)(d)(C)(iv)				All Users	Basic
MP-6 (1)	Operational	MP-06(a)	Media Sanitization | Media Sanitization Documentation			7						9.7.1				164.310(d)(2)(ii)						Technical Users	Basic
MP-6 (2)	Operational	MP-06(b)	Media Sanitization | Equipment Testing	MP-6 (2)		7																Technical Users	Enhanced
MP-7	Operational	MP-07	Media Use	MP-7	3.8.7		8-306 8-310	PI1.6	PI1.6				8.2.3, 8.3.1 & 12.2.1	PR.PT-2								Technical Users	Basic
MP-7 (1)	Operational	MP-07(a)	Media Use | Prohibit Use Without Owner	MP-7 (1)	3.8.8																	Technical Users	Enhanced
N/A	Operational	MP-07(b)	Media Use | Limitations on Use																			Technical Users	Enhanced
MP-8	Operational	MP-08	Media Downgrading				8-310															Technical Users	Enhanced
PE-1	Operational	PE-01	Physical and Environmental Protection Policy & Procedures	PE-1			8-308	A1.2	A1.2	8.2.3 8.2.4			5.1.1, 5.1.2, 6.1.1, 11.1.4, 11.1.5, 12.1.1, 18.1.1 & 18.1.2			164.310(a)(1)						Management	Basic
PE-2	Operational	PE-02	Physical Access Authorizations	PE-2	3.10.1 3.10.2	9	8-308 5-306 5-308 6-104	CC5.5	CC5.5			9.2	9.2.6 & 11.1.2	PR.AC-2		164.310(a)(2)(ii)						Management	Basic
PE-2 (1)	Operational	PE-02(a)	Physical Access Authorizations | Role-Based Physical Access			9										164.310(a)(2)(iii)						Management	Basic

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
PE-2 (2)	Operational	PE-02(b)	Physical Access Authorizations | Identification Requirement			9						9.4 & 9.4.1										Management	Basic
PE-2 (3)	Operational	PE-02(c)	Physical Access Authorizations | Restrict Unescorted Access			9						9.3										Management	Basic
PE-3	Operational	PE-03	Physical Access Control	PE-3	3.10.3 3.10.4 3.10.5	8	5-300 6-104					9.1, 9.1.1, 9.1.2 & 9.2	11.1.1, 11.1.2, 11.1.3 & 11.1.6	PR.AC-2, DE.CM-2, DE.CM-7 & DE.DP-3		164.310(a)(2)(iv)	17.03(2)(g)	622(2)(d)(C)(ii)				Management	Basic
PE-3 (4)	Operational	PE-03(a)	Physical Access Control | Lockable Physical Casings			8																Technical Users	Enhanced
N/A	Operational	PE-03(b)	Physical Access Control | Laptop Storage In Automobiles			8																All Users	Basic
N/A	Operational	PE-03(c)	Physical Access Control | Workstation Security			8																All Users	Basic
N/A	Operational	PE-03(d)	Physical Access Control | Physical Access Logs																			Technical Users	Basic
PE-4	Operational	PE-04	Access Control for Transmission Medium	PE-4	3.10.2		8-605					9.1.2 & 9.1.3	11.1.1, 11.1.2, 11.1.3 & 11.2.3	PR.AC-2				622(2)(d)(C)(ii)				Technical Users	Basic
PE-5	Operational	PE-05	Access Control for Output Devices	PE-5	3.10.1 3.10.2		8-310						11.1.1, 11.1.2 & 11.1.3	PR.AC-2				622(2)(d)(C)(ii)				All Users	Basic
PE-6	Operational	PE-06	Monitoring Physical Access	PE-6	3.10.1 3.10.2	10	5-300					9.1 & 9.1.1	11.1.2 & 12.4.1	PR.[illegible]CM-2, DE.[illegible]RS.AN-1 & RS.CO-3		164.310(c)		622(2)(d)(C)(ii)				Management	Basic
PE-6 (1)	Operational	PE-06(a)	Monitoring Physical Access | Intusion Alarms / Surveillance Equipment	PE-6 (1)		10																Management	Enhanced
PE-7	Operational	PE-07	Visitor Control [withdrawn into PE-2 and PE-3]																			N/A	N/A
PE-8	Operational	PE-08	Visitor Access Records	PE-8		10						9.4.4	11.1.[illegible]					622(2)(d)(C)(ii)				Management	Basic
PE-9	Operational	PE-09	Power Equipment & Power Cabling	PE-9									11.1.4, 11.2.1 & 11.2.3	ID.BE-4 & PR.AC-2								Technical Users	Basic
PE-9 (2)	Operational	PE-09(a)	Power Equipment & Cabling | Automatic Voltage Controls																			Technical Users	Enhanced
PE-10	Operational	PE-10	Emergency Shutoff	PE-10									11.2.2	PR.IP-5								Technical Users	Enhanced
PE-11	Operational	PE-11	Emergency Power	PE-11									11.2.2	ID.BE-4								Technical Users	Enhanced
PE-12	Operational	PE-12	Emergency Lighting	PE-12									11.2.2	PR.IP-5								Technical Users	Enhanced
PE-13	Operational	PE-13	Fire Protection	PE-13									6.1.3, 11.1.4 & 11.2.1	PR.IP-5								Technical Users	Enhanced
PE-13 (1)	Operational	PE-13(a)	Fire Protection | Fire Detection Devices																			Technical Users	Enhanced
PE-13 (2)	Operational	PE-13(b)	Fire Protection | Fire Suppression Devices	PE-13 (2)																		Technical Users	Enhanced
PE-13 (3)	Operational	PE-13(c)	Fire Protection | Automatic Fire Suppression	PE-13 (3)																		Technical Users	Enhanced
PE-14	Operational	PE-14	Temperature & Humidity Controls	PE-14									11.2.1 & 11.2.2	PR.IP-5								Technical Users	Enhanced
PE-14 (2)	Operational	PE-14(a)	Temperature & Humidity Controls | Monitoring With Alarms / Notifications	PE-14 (2)																		Technical Users	Enhanced
PE-15	Operational	PE-15	Water Damage Protection	PE-15									11.1.4 & 11.2.1	PR.IP-5								Technical Users	Enhanced
PE-16	Operational	PE-16	Delivery & Removal	PE-16									11.1.6 & 11.2.5	PR.DS-3				622(2)(d)(C)(ii)				Management	Basic
PE-17	Operational	PE-17	Alternate Work Site	PE-17	3.10.6								6.2.2, 11.2.6 & 13.2.1									Management	Enhanced
PE-18	Operational	PE-18	Location of Information System Components										11.1.4 & 11.2.1	PR.IP-5								Technical Users	Basic
PE-19	Operational	PE-19	Information Leakage			4							11.1.4 & 11.2.1	PR.DS-5								Technical Users	Enhanced
PE-20	Operational	PE-20	Asset Monitoring and Tracking											DE.CM-2 & DE.CM-7								Management	Basic
PS-1	Operational	PS-01	Personnel Security Policy & Procedures	PS-1			8-307						5.1.1, 5.1.2, 6.1.1, 12.1.1, 16.1.2, 18.1.1 & 18.2.2	PR.IP-11								Management	Basic
PS-2	Operational	PS-02	Position Risk Designation (Position Categorization)	PS-2			8-307	CC1.3	CC1.3				6.1.1	PR.IP-11	17.5	164.308(a)(3)(i) & (ii) & (A)						Management	Basic
N/A	Operational	PS-02(a)	Position Risk Designation | Users With Elevated Privileges																			Management	Basic
N/A	Operational	PS-02(b)	Position Risk Designation | Security-Related Positions								500.10											Management	Basic
PS-3	Operational	PS-03	Personnel Screening	PS-3	3.9.1 3.9.2		8-103 8-104 8-307					12.7	7.1.1	PR.DS-5 & PR.IP-11		164.308(a)(3)(ii) & (B)						Management	Basic
PS-3 (3)	Operational	PS-03(a)	Personnel Screening | Information With Special Protection Measures	PS-3 (3)																		Management	Enhanced
PS-4	Operational	PS-04	Personnel Termination	PS-4	3.9.1 3.9.2		8-303 5-309					9.3	7.3.1, 8.1.4 & 9.2.6	PR.IP-11		164.308(a)(3)(ii) & (C)	17.03(2)(e)					Management	Basic
N/A	Operational	PS-04(a)	Personnel Termination | Asset Collection																			Management	Basic
N/A	Operational	PS-04(b)	Personnel Termination | High Risk Terminations																			Management	Basic
PS-5	Operational	PS-05	Personnel Transfer	PS-5	3.9.1 3.9.2		8-303 5-309						7.3.1, 8.1.4 & 9.2.6	PR.IP-11								Management	Basic

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
PS-6	Operational	PS-06	Access Agreements	PS-6			8-103 8-104 8-105						13.2.4, 15.1.2, 8.1.3, 6.1.1, 7.1.2, 7.2.1, 13.2.1, 6.2.1 & 6.2.2	PR.DS-5 & PR.IP-11		164.308(a)(4)(i)						Management	Basic
PS-7	Operational	PS-07	Third-Party Personnel Security	PS-7			8-304						6.1.1, 15.1.2 & 7.2.1	ID.AM-6, ID.GV-2, PR.AT-3 & PR.IP-11								Management	Basic
PS-8	Operational	PS-08	Personnel Sanctions	PS-8			1-304						7.2.3	PR.IP-11		164.308(a)(1)(ii)(C)	17.03(2)(d)					Management	Basic
N/A	Operational	PS-08(a)	Personnel Sanctions | Workplace Investigations																X			Management	Basic
AC-1	Technical	AC-01	Access Control Policy & Procedures	AC-1			8-101 8-606	CC5.1	CC5.1	8.2.2		8.1 & 8.4	5.1.1, 5.1.2, 6.1.1, 12.1.1, 13.2.1, 9.1.1, 11.2.9, 9.1.2, 9.4.[illegible] 6.2.1, 6.2.2, 18.1.1 & 18.[illegible]			164.312(a)(1)						Management	Basic
AC-2	Technical	AC-02	Account Management	AC-2	3.1.1 3.1.2	1	8-606			8.2.2		8.1.3-8.1.5, 8.2.2, 8.5, 8.5.1, 8.6 & 8.7	[illegible]2.1, 9.2.2, 9.2.3, [illegible]2.5 & 9.2.6	DE.[illegible]	16.9	164.312(d)	17.04(1(a)					Management	Basic
AC-2 (1)	Technical	AC-02(a)	Account Management | Automated System Account Management	AC-2 (1)																		Technical Users	Enhanced
AC-2 (2)	Technical	AC-02(b)	Account Management | Removal of Temporary / Emergency Accounts	AC-2 (2)																	2-1	Technical Users	Enhanced
AC-2 (3)	Technical	AC-02(c)	Account Management | Disable Inactive Accounts	AC-2 (3)																	2-1 3-7	Technical Users	Enhanced
AC-2 (4)	Technical	AC-02(d)	Account Management | Automated Audit Actions	AC-2 (4)																		Technical Users	Enhanced
AC-2 (5)	Technical	AC-02(e)	Account Management | Inactivity Logout	AC-2 (5)																		Technical Users	Basic
AC-2 (7)	Technical	AC-02(f)	Account Management | Role-Based Schemes (Role Based Access Control (RBAC))	AC-2 (7)		1						[illegible]1.1-7.1.4, 7.2, 7.2.1 & 7.2.3+K316D312G316:I316D312G316:I316G316:Q31G316:Q316				164.308(a)(4(ii)(A) & (B) &(C)					3-1	Management	Basic
AC-2 (10)	Technical	AC-02(g)	Account Management | Restrictions on Shared Groups / Accounts	AC-2 (10)																		Technical Users	Basic
AC-2 (12)	Technical	AC-02(h)	Account Management | Shared / Group Account Credential Termination	AC-2 (12)																		Technical Users	Basic
AC-3	Technical	AC-03	Access Enforcement	AC-3	3.1.1 3.1.2	6	606					7.1, 7.1.1-7.1.4, 7.2, 7.2.1 & 7.2.3	6.2.2, 9.1.2, 9.4.1, 9.4.4, 9.4.5, 13.1.1, 14.1.2, 14.1.3 & 18.1.3	PR.AM-3, PR.AC-4 & PR.PT-3		164.308(a)(4(i) & (ii)	17.04(1)(b) & 17.04(2)(a)	622(2)(d)(C)(iii)				Management	Basic
AC-4	Technical	AC-04	Information Flow Enforcement (Access Control Lists)	AC-4	3.1.3	11						1.1.6, 1.3.3, 1.3.5 & 1.3.6	8.2.2, 8.2.3, 13.2.1, 13.1.3, 14.1.2 & 14.1.3	PR.AC-5, PR.DS-5, PR.PT-4 & DE.AE-1	13.3 13.6 13.8 13.9			622(2)(d)(C)(iii)				Technical Users	Basic
AC-4 (1)	Technical	AC-04(a)	Information Flow Enforcement | Object Security Atributes												13.3							Technical Users	Basic
AC-4 (4)	Technical	AC-04(b)	Information Flow Enforcement | Content Check For Encrypted Data												13.7							Technical Users	Enhanced
AC-4 (5)	Technical	AC-04(c)	Information Flow Enforcement | Embedded Data Types												13.3							Technical Users	Enhanced
AC-4 (6)	Technical	AC-04(d)	Information Flow Enforcement | Metadata																			Technical Users	Enhanced
AC-4 (9)	Technical	AC-04(e)	Information Flow Enforcement | Human Reviews									1.1.7									1-4	Technical Users	Enhanced
AC-4 (21)	Technical	AC-04(f)	Information Flow Enforcement | Physical / Logial Separation of Information Flows	AC-4 (21)		11																Technical Users	Enhanced
AC-5	Technical	AC-05	Separation of Duties	AC-5	3.1.4		8-611					6.4.2	6.1.2	PR.AC-4 & PR.DS-5								Management	Enhanced
AC-6	Technical	AC-06	Least Privilege	AC-6	3.1.5	2, 5	8-303	CC5.6	CC5.6				9.1.2, 9.2.3, 9.4.4 & 9.4.5	PR.AC-4 & PR.DS-5	5.1			622(2)(d)(C)(iii)			3-2 3-7	Management	Basic
AC-6 (1)	Technical	AC-06(a)	Auditable Events | Authorize Access to Security Functions	AC-6 (1)	3.1.5																	Technical Users	Basic
AC-6 (2)	Technical	AC-06(b)	Auditable Events | Non-Privileged Access for Non-Security Functions	AC-6 (2)	3.1.6							10.2 & 10.2.1-10.2.7									3-2	Technical Users	Basic
AC-6 (5)	Technical	AC-06(c)	Auditable Events | Privileged Accounts	AC-6 (5)	3.1.5																3-2 3-3 3-4	Technical Users	Basic
AC-6 (9)	Technical	AC-06(d)	Auditable Events | Auditing Use of Privileged Functions	AC-6 (9)	3.1.7							10.2 & 10.2.1-10.2.7			5.2						3-3	Technical Users	Basic

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
AC-6 (10)	Technical	AC-06(e)	Auditable Events | Prohibit Non-Privileged Users from Executing Privileged Functions	AC-6 (10)	3.1.7																3-2 3-4	Technical Users	Basic
AC-7	Technical	AC-07	Unsuccessful Login Attempts	AC-7	3.1.8		8-609					8.1.6 & 8.1.7	9.4.2		5.5		17.04(1)(e)					Management	Basic
AC-7 (2)	Technical	AC-07(a)	Unsuccessful Login Attempts | Mobile Device Purging																			Management	Basic
AC-8	Technical	AC-08	System Use Notification (Logon Banner)	AC-8	3.1.9		8-609						9.4.2									Technical Users	Basic
N/A	Technical	AC-08(a)	System Use Notification | Standardized Microsoft Windows Banner																			Technical Users	Enhanced
N/A	Technical	AC-08(b)	System Use Notification | Truncated Banner																			Technical Users	Enhanced
AC-9	Technical	AC-09	Previous Logon Notification				8-609						9.4.2									Technical Users	Enhanced
AC-10	Technical	AC-10	Concurrent Session Control	AC-10			8-609															Technical Users	Basic
AC-11	Technical	AC-11	Screen Lock	AC-11	3.1.10		8-609						9.4.2, 11.2.8 & 11.2.9		16.5							Technical Users	Basic
AC-11 (1)	Technical	AC-11(a)	Screen Lock | Pattern Hiding Displays	AC-11 (1)	3.1.10																	Technical Users	Basic
AC-12	Technical	AC-12	Session Termination	AC-12	3.1.11		8-311 8-609					8.1.8	9.4.2			164.312(a)(2)(iii)						Technical Users	Basic
AC-13	Technical	AC-13	Account Restriction Parameters									10.6, 10.6.1 & 10.6.2										Technical Users	Enhanced
AC-14	Technical	AC-14	Permitted Actions Without Identification or Authentication	AC-14			8-501 8-504 8-505															Technical Users	Basic
AC-15	Technical	AC-15	Automated Marking																			Technical Users	Enhanced
AC-16	Technical	AC-16	Security Attributes				8-306						8.2	PR.AC-4								Technical Users	Enhanced
AC-17	Technical	AC-17	Remote Access	AC-17	3.1.1 3.1.2								6.2.1 & 6 13.1.1, 13.2.1 & 14.1.2	PR.AC-3 & PR.PT-4								All Users	Basic
AC-17 (1)	Technical	AC-17(a)	Remote Access | Automated Monitoring / Control	AC-17 (1)	3.1.12																	All Users	Enhanced
AC-17 (2)	Technical	AC-17(b)	Remote Access | Protection of Confidentiality / Integrity Using Encryption	AC-17 (2)	3.1.13																	All Users	Enhanced
AC-17 (3)	Technical	AC-17(c)	Remote Access | Managed Access Control Points	AC-17 (3)	3.1.14																1-5	All Users	Enhanced
AC-17 (4)	Technical	AC-17(d)	Remote Access | Privileged Commands & Access	AC-17 (4)	3.1.15	5															1-5	Management	Basic
AC-17 (9)	Technical	AC-17(e)	Remote Access | Disconnect / Disable Remote Access	AC-17 (9)																		Technical Users	Enhanced
N/A	Technical	AC-17(e)	Remote Access | Telecommuting																			All Users	Basic
N/A	Technical	AC-17(f)	Remote Access | Monitoring Vendor Usage									8.1.5										All Users	Basic
AC-18	Technical	AC-18	Wireless Access	AC-18	3.1.16								6.2.1. 13.1.1 & 13.2.1	PR.PT-4	15.1 15.2 15.3 15.4 15.5 15.6 15.7 15.8 15.9							Management	Basic
AC-18 (1)	Technical	AC-18(a)	Wireless Access | Authentication & Encryption	AC-18 (1)	3.1.17							4.1.1										Technical Users	Basic
AC-18 (3)	Technical	AC-18(b)	Wireless Access | Disable Wireless Networking																			Technical Users	Enhanced
AC-18 (4)	Technical	AC-18(c)	Wireless Access | Restrict Configuration By Users												15.4 15.7							Technical Users	Enhanced
AC-18 (5)	Technical	AC-18(d)	Wireless Access | Configure Wireless Communications																			Technical Users	Basic
AC-19	Technical	AC-19	Access Control For Mobile Devices	AC-19	3.1.18		8-610						6.2.1, 8.2.3, 11.2.6 & 13.2.1	PR.AC-3								All Users	Basic
AC-19 (5)	Technical	AC-19(a)	Access Control For Mobile Devices | Full Device / Container-Based Encryption	AC-19 (5)	3.1.19						500.15											All Users	Enhanced
N/A	Technical	AC-19(b)	Access Control For Mobile Devices | Central Management Of Mobile Devices																			Technical Users	Basic
N/A	Technical	AC-19(c)	Access Control For Mobile Devices | Remote Purging																			Technical Users	Basic
N/A	Technical	AC-19(d)	Access Control For Mobile Devices | Personally Owned Devices																			All Users	Basic
N/A	Technical	AC-19(e)	Access Control For Mobile Devices | Tamper Protection & Detection																			All Users	Basic
AC-20	Technical	AC-20	Use of External Information Systems	AC-20	3.1.20		8-700						8.1.3, 9.1.2, 11.2.6, 13.1.1 & 13.2.1	ID.AM-4 & PR.AC-3								All Users	Basic
AC-20 (1)	Technical	AC-20(a)	Use of External Information Systems | Limits of Authorized Use	AC-20 (1)	3.1.20																	All Users	Basic
AC-20 (2)	Technical	AC-20(b)	Use of External Information Systems | Portable Storage Devices	AC-20 (2)	3.1.21																	All Users	Basic
AC-21	Technical	AC-21	Information Sharing	AC-21				C1.3	C1.3					PR.IP-8								Technical Users	Basic

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
AC-22	Technical	AC-22	Publicly Accessible Content	AC-22	3.1.22								14.1.2 & 9.4.1									Technical Users	Basic
AC-23	Technical	AC-23	Data Mining Protection																			Technical Users	Enhanced
AC-24	Technical	AC-24	Access Control Decisions										9.4.1									Management	Basic
AC-25	Technical	AC-25	Reference Monitor																			Technical Users	Enhanced
AU-1	Technical	AU-01	Audit and Accountability Policy & Procedures	AU-1			8-602				500.06	10.1 & 10.8	5.1.1, 5.1.2, 6.1.1, 12.1.1, 18.1.1, 18.2.2 & 12.7.1	PR.PT-1		164.312(b)						Management	Basic
AU-2	Technical	AU-02	Auditable Events	AU-2	3.3.1 3.3.2		8-602				500.06		12.4.1, 12.4.3, 9.4.4 & 12.7.1	PR.PT-1			17.04(4)	622(2)(d)(B)(iii)				Management	Basic
AU-2 (3)	Technical	AU-02(a)	Auditable Events | Reviews & Updates	AU-2 (3)	3.3.3						500.06	10.2 & 10.2.1-10.2.7										Technical Users	Basic
AU-3	Technical	AU-03	Content of Audit Records	AU-3	3.3.1 3.3.2		8-602				500.06	10.3 & 10.3.1-10.3.6	12.4.1 & 12.4.3	[illegible]R.PT-1								Technical Users	Enhanced
AU-3 (1)	Technical	AU-03(a)	Content Of Audit Records | Additional Audit Information	AU-3 (1)	3.3.1 3.3.2																	Technical Users	Basic
AU-4	Technical	AU-04	Audit Storage Capacity	AU-4			8-602						12.1.3, 12.4.2 & 12.4.3	[illegible] & PR.PT-1								Technical Users	Basic
AU-4 (1)	Technical	AU-04(a)	Audit Storage Capacity | Transfer To Alternate Storage																			Technical Users	Basic
AU-5	Technical	AU-05	Response to Audit Processing Failures	AU-5	3.3.4		8-602						[illegible]3, 12.4.2 & [illegible]4.3									Technical Users	Basic
AU-5 (2)	Technical	AU-05(a)	Response To Audit Processing Failures | Real-Time Alerts																			Technical Users	Enhanced
AU-6	Technical	AU-06	Audit Review, Analysis & Reporting	AU-6	3.3.1 3.3.2		8-602						12.4.1, 16.1.2 & 16.1.4	PR.PT-1, DE.AE-2, DE.AE-3, DE.DP-4, RS.AN-1 & RS.CO-2	16.1 16.2 16.3 16.4 16.8							Technical Users	Basic
AU-6 (1)	Technical	AU-06(a)	Audit Review, Analysis & Reporting | Process Integration	AU-6 (1)																		Technical Users	Enhanced
AU-6 (3)	Technical	AU-06(b)	Audit Review, Analysis & Reporting | Correlate Audit Repositories	AU-6 (3)	3.3.5																	Technical Users	Enhanced
AU-6 (8)	Technical	AU-06(c)	Audit Review, Analysis & Reporting | Full Text Analysis Of Privileged Commands																			Technical Users	Enhanced
AU-7	Technical	AU-07	Audit Reduction & Report Generation	AU-7	3.3.6		8-602						12.4.1 & 16.1.7	PR.PT-1 & RS.AN-3								Technical Users	Enhanced
AU-7 (1)	Technical	AU-07(a)	Audit Reduction & Report Generation | Automatic Processing	AU-7 (1)																		Technical Users	Enhanced
AU-8	Technical	AU-08	Time Stamps	AU-8	3.3.7		8-602					10.4 & 10.4.1-10.4.5	12.4.4	PR.PT-1	6.1							Technical Users	Basic
AU-8 (1)	Technical	AU-08(a)	Time Stamps | Synchronization With Authoritative Time Source	AU-8 (1)	3.3.7																	Technical Users	Basic
AU-9	Technical	AU-09	Protection of Audit Information	AU-9	3.3.8		[illegible]					10.5 & 10.5.1-10.5.5	12.4.2, 12.4.3, 16.1.7 & 18.1.3	PR.PT-1		164.312(c)(1)						Technical Users	Basic
AU-9 (2)	Technical	AU-09(a)	Protection of Audit Information | Audit Backup on Separate Physical Systems / Components	AU-9 (2)																		Technical Users	Enhanced
AU-9 (4)	Technical	AU-09(b)	Protection of Audit Information | Access by Subset of Privileged Users		3.3.9																	Technical Users	Enhanced
AU-10	Technical	AU-10	Non-Repudiation				8-602						13.2.3, 14.1.2 & 14.1.3	PR.PT-1		164.312(c)(2)						Technical Users	Enhanced
AU-11	Technical	AU-11	Audit Record Retention	AU-11	3.3.1		8-602				500.13	10.7	12.4.1, 16.1.7 & 18.1.3	PR.PT-1								Technical Users	Basic
AU-12	Technical	AU-12	Audit Generation	AU-12	3.3.1 3.3.2		8-602						12.4.1 & 12.4.3	PR.PT-1, DE.CM-1, DE.CM-3 & DE.CM-7								Technical Users	Basic
AU-13	Technical	AU-13	Monitoring for Information Disclosure				8-602							PR.PT-1 & DE.CM-3			17.04(3)					Management	Basic
AU-14	Technical	AU-14	Session Audit				8-602						12.4.1	PR.PT-1								Technical Users	Enhanced
AU-15	Technical	AU-15	Alternate Audit Capability				8-602							PR.PT-1								Technical Users	Enhanced
AU-16	Technical	AU-16	Cross-Organizational Auditing				8-602							PR.PT-1								Management	Enhanced
CM-1	Technical	CM-01	Configuration Management Policy & Procedures	CM-1			8-311 8-610						5.1.1, 5.1.2, 6.1.1, 12.1.1, 15.5.1, 14.2.2, 18.1.1 & 18.2.2									Management	Basic
CM-2	Technical	CM-02	Baseline Configurations	CM-2	3.4.1 3.4.2		8-202 8-311 8-610					1.1.1	12.1.2, 12.1.4 & 12.5.1	PR.DS-7, PR.IP-1 & DE.AE-1	3.1 3.2 5.3 5.4						2-3 2-4	Technical Users	Basic
CM-2 (1)	Technical	CM-02(a)	Baseline Configuration | Reviews & Updates	CM-2 (1)											11.1							Technical Users	Basic

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
CM-2 (2)	Technical	CM-02(b)	Baseline Configuration | Automation Support for Accuracy / Currency	CM-2 (2)																		Technical Users	Enhanced
CM-2 (3)	Technical	CM-02(c)	Baseline Configuration | Retention Of Previous Configurations	CM-2 (3)																		Technical Users	Basic
CM-2 (6)	Technical	CM-02(d)	Baseline Configuration | Development & Test Environments									6.4.1										Technical Users	Basic
CM-2 (7)	Technical	CM-02(e)	Baseline Configuration | Configure Systems, Components or Devices for High-Risk Areas	CM-2 (7)																		Technical Users	Enhanced
N/A	Technical	CM-02(f)	Baseline Configuration | Configuration File Synchronization									1.2.2										Technical Users	Basic
CM-3	Technical	CM-03	Configuration Change Control	CM-3	3.4.3		8-103 8-104 8-311 8-610	CC7.3	CC7.3				12.1.2, 14.2.9, 12.2.1, 12.3.1, 14.2.2, 14.2.3 & 14.2.4	PR.IP-1, PR.IP-3, DE.CM-1 & DE.CM-7								Technical Users	Basic
CM-3 (1)	Technical	CM-03(a)	Configuration Change Control | Prohibition Of Changes																			Technical Users	Basic
CM-3 (2)	Technical	CM-03(b)	Configuration Change Control | Test, Validate & Document Changes					CC7.4	CC7.4						11.2							Technical Users	Basic
CM-3 (4)	Technical	CM-03(c)	Configuration Change Control | Security Representative						CC3.3	1.2.6												Technical Users	Basic
CM-4	Technical	CM-04	Security Impact Analysis	CM-4	3.4.4		8-103 8-104 8-311 8-610			1.2.6		6.4, 6.4.5, 6.4.5.1-	12.1.2, 12.1.4, 12.2.1, 14.2.3 14.2.4	PI								Technical Users	Basic
CM-5	Technical	CM-05	Access Restrictions for Change	CM-5	3.4.5		8-311 8-610						9.2.3, 12.1.4 12 & 12.5.1	PR.IP-1								Technical Users	Basic
CM-5 (1)	Technical	CM-05(a)	Access Restrictions For Change | Automated Access Enforcement / Auditing	CM-5 (1)																		Technical Users	Enhanced
CM-5 (3)	Technical	CM-05(b)	Access Restrictions For Change | Signed Components	CM-5 (3)																		Technical Users	Enhanced
CM-5 (4)	Technical	CM-05(c)	Access Restrictions For Change | Two-Person Rule																			Technical Users	Enhanced
CM-5 (5)	Technical	CM-05(d)	Access Restrictions For Change | Limit Production / Operational Privliges	CM-5 (5)																		Technical Users	Enhanced
CM-5 (6)	Technical	CM-05(e)	Access Restrictions For Change | Library Privileges																			Technical Users	Enhanced
CM-6	Technical	CM-06	Configuration Settings	CM-6	3.4.1 3.4.2		8-202 8-311					1.1 & 1.1.1	12.4.1	PR.IP-1	3.3 3.5							Technical Users	Basic
CM-6 (1)	Technical	CM-06(a)	Configuration Settings | Automated Central Management / Application / Verification	CM-6 (1)											3.6 11.3							Technical Users	Enhanced
CM-6 (2)	Technical	CM-06(b)	Configuration Settings | Respond To Unauthorized Changes												3.7							Technical Users	Basic
CM-7	Technical	CM-07	Least Functionality	CM-7	3.4.6	2						1.1.5, 1.2.1, 2.2.2, 2.2..4 & 2.2.5	9.1.2, 12.4.1 & 12.5.1	PR.IP-1	9.1 12.1		17.03(2)(a)				1-3	Technical Users	Basic
CM-7 (1)	Technical	CM-07(a)	Least Functionality | Periodic Review	CM-7 (1)	3.4.7																1-4	Technical Users	Basic
CM-7 (2)	Technical	CM-07(b)	Least Functionality | Prevent Program Execution	CM-7 (2)	3.4.7										2.1						1-3	Technical Users	Basic
CM-7 (4)(5)	Technical	CM-07(c)	Least Functionality | Unauthorized or Authorized Software / Whitelisting	CM-7 (5)	3.4.8										2.2							Technical Users	Enhanced
CM-8	Technical	CM-08	Information System Component Inventory	CM-8	3.4.1 3.4.2							1.1.2	8.1.1 & 8.1.2	ID.AM-1, ID.AM-2, PR.DS-3, PR.PT-3 & DE.CM-7	2.3	164.310(d)(2)(iii)					Technical Users	Basic
CM-8 (1)	Technical	CM-08(a)	Information System Component Inventory | Updates During Installation / Removals	CM-8 (1)	3.4.1 3.4.2																	Technical Users	Enhanced
CM-8 (3)	Technical	CM-08(b)	Information System Component Inventory | Automated Unauthorized Component Detection	CM-8 (3)																		Technical Users	Enhanced
CM-8 (5)	Technical	CM-08(c)	Information System Component Inventory | No Duplicate Accounting of Components	CM-8 (5)																		Technical Users	Enhanced
CM-8 (6)	Technical	CM-08(d)	Information System Component Inventory | Approved Deviations																			Management	Basic
N/A	Technical	CM-08(e)	Information System Component Inventory | Network Diagrams									1.1.2 & 1.1.3										Technical Users	Basic
N/A	Technical	CM-08(f)	Information System Component Inventory | Network Access Control (NAC)																			Technical Users	Enhanced
CM-9	Technical	CM-09	Configuration Management Plan	CM-9				CC2.6	CC2.6			1.1.5	14.2.4	PR.IP-1								Technical Users	Basic
CM-10	Technical	CM-10	Software Usage Restrictions	CM-10									12.5.1 & 18.1.2	DE.CM-3								Management	Basic
CM-10 (1)	Technical	CM-10(a)	Software Usage Restrictions | Open Source Software	CM-10 (1)																		Technical Users	Enhanced
CM-11	Technical	CM-11	User-Installed Software	CM-11	3.4.9								12.2.1, 12.4.1, 12.5.1 & 12.6.2	DE.CM-3								Management	Basic
CM-11 (1)	Technical	CM-11(a)	User-Installed Software | Unauthorized Installation Alerts																			Technical Users	Enhanced

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
CM-11 (2)	Technical	CM-11(b)	User-Installed Software | Prohibit Installation Without Privileged Status																			Technical Users	Enhanced
IA-1	Technical	IA-01	Identification & Authentication Policy & Procedures	IA-1			8-607	CC5.1	CC5.1		500.07	8.1	5.1.1, 5.1.2, 6.1.1, 12.1.1, 18.1.1 & 18.2.2									Management	Basic
IA-2	Technical	IA-02	Identification and Authentication	IA-2	3.5.1 3.5.2	6	8-607	CC5.3	CC5.3		500.07	8.1.1 & 8.2	14.1.2, 14.1.3, 9.4.2 & 9.2.1				17.04(1)(c) & 17.04(2)(b)					All Users	Basic
IA-2 (1)	Technical	IA-02(a)	Identification & Authentication | Network Access to Privileged Accounts	IA-2 (1)	3.5.3																	Technical Users	Enhanced
IA-2 (2)	Technical	IA-02(b)	Identification & Authentication | Network Access to Non-Privileged Accounts	IA-2 (2)	3.5.3																	Technical Users	Enhanced
IA-2 (3)	Technical	IA-02(c)	Identification & Authentication | Local Access to Privileged Accounts	IA-2 (3)	3.5.3																	Technical Users	Enhanced
IA-2 (5)	Technical	IA-02(d)	Identification & Authentication | Group Authentication	IA-2 (5)																		Technical Users	Enhanced
IA-2 (8)	Technical	IA-02(e)	Identification & Authentication | Network Access to Privileged Accounts - Replay Resistant	IA-2 (8)	3.5.4																	Technical Users	Enhanced
IA-2 (9)	Technical	IA-02(f)	Identification & Authentication | Network Access to Non-Privileged Accounts - Replay Resistant		3.5.4																	Technical Users	Enhanced
IA-2 (11)	Technical	IA-02(g)	Identification & Authentication | Remote Access - Separate Device (Multifactor Authentication)	IA-2 (11)							500.12				5.6 5.7 16.11 16.12							Technical Users	Enhanced
IA-2 (12)	Technical	IA-02(h)	Identification & Authentication | Acceptance of PIV Credentials	IA-2 (12)																		Technical Users	Enhanced
IA-3	Technical	IA-03	Device Identification & Authentication	IA-3	3.5.1	5	8-607															All Users	Basic
IA-4	Technical	IA-04	Identifier Management (User Names)	IA-4	3.5.5 3.5.6		8-607						9.2.1 & 9.2.2			164.312(a)(2)(i)	17.04(1)(d)					All Users	Basic
IA-4 (4)	Technical	IA-04(a)	Identifier Management | Identify User Status	IA-4 (4)																		Technical Users	Enhanced
IA-4 (5)	Technical	IA-04(b)	Identifier Management | Dynamic Management																			Technical Users	Enhanced
IA-4 (6)	Technical	IA-04(c)	Identifier Management | Cross-Organization Management																			Technical Users	Enhanced
N/A	Technical	IA-04(d)	Identifier Management | Privileged Account Identifiers																			All Users	Basic
IA-5	Technical	IA-05	Authenticator Management (Passwords)	IA-5	3.5.1 3.5.2	6	8-607					8.1.2, 8.2.3, 8.2.4 & 8.2.5	9.2.1, 9.2.2, 9.2.4, 9.3.1, 9.4.2 & 9.4.3			164.308(a)(5)(ii)(D)	17.04(1)(b)-(e) & 17.04(2)(b)				3-5 3-6	All Users	Basic
IA-5 (1)	Technical	IA-05(a)	Authenticator Management | Password-Based Authentication	IA-5 (1)	3.5.7 3.5.8 3.5.9 3.5.10	6						8.1.2, 8.2.3, 8.2.4 & 8.2.5	9.2.1, 9.2.2, 9.2.4, 9.3.1, 9.4.2 & 9.4.3			164.308(a)(5)(ii)(D)	17.04(1)(b)-(e) & 17.04(2)(b)					Technical Users	Basic
IA-5 (2)	Technical	IA-05(b)	Authenticator Management | PKI-Based Authentication	IA-5 (2)		6																Technical Users	Enhanced
IA-5 (3)	Technical	IA-05(c)	Authenticator Management | In-Person or Trusted Third-Party Registration	IA-5 (3)																		Technical Users	Enhanced
IA-5 (4)	Technical	IA-05(d)	Authenticator Management | Automated Support For Password Strength	IA-5 (4)																		Technical Users	Enhanced
IA-5 (6)	Technical	IA-05(e)	Authenticator Management | Protection of Authenticators	IA-5 (6)																		Technical Users	Enhanced
IA-5 (7)	Technical	IA-05(f)	Authenticator Management | No Embedded Unencrypted Static Authenticators	IA-5 (7)																		Technical Users	Enhanced
IA-5 (11)	Technical	IA-05(g)	Authenticator Management | Hardware Token-Based Authentication	IA-5 (11)																		Technical Users	Enhanced
N/A	Technical	IA-05(h)	Authenticator Management | Vendor-Supplied Defaults									2.1, 2.1.1 & 8.3									1-1 2-1 2-2	Technical Users	Basic
IA-6	Technical	IA-06	Authenticator Feedback	IA-6	3.5.11		8-607						9.4.2 & 9.4.3									Technical Users	Enhanced
IA-7	Technical	IA-07	Cryptographic Module Authentication	IA-7			8-607					8.2.1	18.1.5		16.13 16.14							Technical Users	Basic
IA-8	Technical	IA-08	Identification & Authentication (Non-Organizational Users)	IA-8			8-607	CC5.3	CC5.3				14.1.2, 14.1.3, 9.4.2 & 9.2.1									Technical Users	Basic
IA-8 (1)	Technical	IA-08(a)	Identification & Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies	IA-8 (1)																		Technical Users	Enhanced
IA-8 (2)	Technical	IA-08(b)	Identification & Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials	IA-8 (2)																		Technical Users	Enhanced
IA-8 (3)	Technical	IA-08(c)	Identification & Authentication (Non-Organizational Users) | Use of FICAM-Approved Products	IA-8 (3)																		Technical Users	Enhanced
IA-8 (4)	Technical	IA-08(d)	Identification & Authentication (Non-Organizational Users) | Use of FICAM-Issued Profiles	IA-8 (4)																		Technical Users	Enhanced
IA-9	Technical	IA-09	Service Provider Identification & Authentication (Vendors)				8-607															Technical Users	Enhanced
IA-10	Technical	IA-10	Adaptive Identification and Authentication				8-607															Technical Users	Enhanced
IA-11	Technical	IA-11	Re-Authentication				8-607					8.1.8										Technical Users	Enhanced

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
MA-1	Technical	MA-01	Maintenance Policy & Procedures	MA-1			8-304						5.1.1, 5.1.2, 6.1.1, 12.1.1, 16.1.2, 18.1.1 & 18.2.2			164.310(a)(2)(iv)						Management	Basic
MA-2	Technical	MA-02	Controlled Maintenance	MA-2	3.7.1 3.7.2 3.7.3		8-304						11.2.4 & 11.2.5	PR.MA-1								Technical Users	Basic
N/A	Technical	MA-02(a)	Controlled Maintenance | Maintenance Activities																			Technical Users	Enhanced
MA-3	Technical	MA-03	Maintenance Tools	MA-3	3.7.1 3.7.2		8-304						11.2.4 & 12.2.1	PR.MA-1								Technical Users	Basic
MA-3 (1)	Technical	MA-03(a)	Maintenance Tools | Inspect Tools	MA-3 (1)	3.7.1 3.7.2								11.2.4 & 12.2.1	PR.MA-1								Technical Users	Enhanced
MA-3 (2)	Technical	MA-03(b)	Maintenance Tools | Inspect Media	MA-3 (2)	3.7.1 3.7.2 3.7.4																	Technical Users	Enhanced
MA-3 (3)	Technical	MA-03(c)	Maintenance Tools | Prevent Unauthorized Removal	MA-3 (3)																		Technical Users	Basic
MA-4	Technical	MA-04	Non-Local Maintenance	MA-4	3.7.5								11.2.4		2							Technical Users	Basic
MA-4 (1)	Technical	MA-04(a)	Non-Local Maintenance | Auditing																			Technical Users	Enhanced
MA-4 (2)	Technical	MA-04(b)	Non-Local Maintenance | Document Non-Local Maintenance	MA-4 (2)																		Technical Users	Basic
MA-4 (6)	Technical	MA-04(c)	Non-Local Maintenance | Cryptographic Protection												3.4							Technical Users	Basic
MA-4 (7)	Technical	MA-04(d)	Non-Local Maintenance | Remote Disconnect Verification																			Technical Users	Enhanced
MA-5	Technical	MA-05	Maintenance Personnel	MA-5	3.7.6		8-304						9.4.5, 11.	PR.MA-1								Technical Users	Basic
MA-5 (1)	Technical	MA-05(a)	Maintenance Personnel | Individuals Without Appropriate Access	MA-5 (1)																		Management	Enhanced
MA-6	Technical	MA-06	Timely Maintenance	MA-6			8-304						11.2.4									Technical Users	Basic
SC-1	Technical	SC-01	System & Communications Protection Policy & Procedures	SC-1			8-101 8-605						5.1.1, 5.1.2, 6.1.1, 12.1.1, 13.2.1, 9.1.2, 10.1.1, 18.1.1 & 18.2.2									Management	Basic
SC-2	Technical	SC-02	Application Partitioning	SC-2	3.13.3							11.3.4	12.2.1, 14.1.3, 13.1.3 & 9.4.4		2.4							Technical Users	Enhanced
SC-3	Technical	SC-03	Security Function Isolation				8-105					1.2, 1.3.1, 2.2.1 & 11.3.4	12.2.1 & 14.1.3		14.1 14.2 14.3 14.4 14.5 14.6 14.7							Technical Users	Basic
SC-3 (5)	Technical	SC-03(a)	Security Function Isolation | Layered Defenses									1.3.7										Technical Users	Basic
SC-4	Technical	SC-04	Information In Shared Resources	SC-4	3.13.4																	Technical Users	Basic
SC-5	Technical	SC-05	Denial of Service (DoS) Protection	SC-5			8-70	.1	A1.1				12.1.3 & 13.1.1	PR.DS-4 & DE.CM-1								Technical Users	Enhanced
SC-6	Technical	SC-06	Resource Priority	SC-6																		Technical Users	Enhanced
SC-7	Technical	SC-07	Boundary Protection	SC-7	3.13.1 3.13.2 3.13.5		8-701					1.1.3, 1.1.4, 1.2.1, 1.2.3 & 1.3	9.1.2, 12.2.1, 12.2.1, 12.4.1, 13.1.1, 13.1.3, 13.2.1, 13.2.3, 14.1.2, & 14.1.3	PR.AC-5, PR.DS-5, PR.PT-4 & DE.CM-1			17.04(6)					Technical Users	Basic
SC-7 (3)	Technical	SC-07(a)	Boundary Protection | Access Points	SC-7 (3)																		Technical Users	Basic
SC-7 (4)	Technical	SC-07(b)	Boundary Protection | External Telecommunications Services	SC-7 (4)																		Technical Users	Basic
SC-7 (5)	Technical	SC-07(c)	Boundary Protection | Deny Traffic by Default & Allow Traffic by Exception	SC-7 (5)	3.13.6							1.2.1									1-2	Technical Users	Basic
SC-7 (7)	Technical	SC-07(d)	Boundary Protection | Prevent Split Tunneling for Remote Devices	SC-7 (7)	3.13.7																	Technical Users	Enhanced
SC-7 (8)	Technical	SC-07(e)	Boundary Protection | Route Traffic To Proxy Servers	SC-7 (8)								1.3										Technical Users	Basic
SC-7 (12)	Technical	SC-07(f)	Boundary Protection | Host-Based Protection	SC-7 (12)								1.4										Technical Users	Basic
SC-7 (13)	Technical	SC-07(g)	Boundary Protection | Isolation of Security Tools / Mechanisms / Support Components	SC-7 (13)																		Technical Users	Enhanced
SC-7 (18)	Technical	SC-07(h)	Boundary Protection | Internal Network Address Space									1.3.8										Technical Users	Basic
N/A	Technical	SC-07(i)	Boundary Protection | Fail Secure	SC-7 (18)										PR.PT-5								Technical Users	Enhanced
SC-8	Technical	SC-08	Transmission Confidentiality & Integrity	SC-8	3.13.8		8-605			8.2.5	500.15	4.1	8.2.3, 13.1.1, 13.2.1, 13.2.3, 14.1.2 & 14.1.3	PR.DS-2 & PR.DS-5		164.312(e)(2)(i), 164.312(e)(1) & 164.312(e)(2)(ii)	17.04(3)	622(2)(d)(C)(iii)				Technical Users	Basic

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
SC-8 (1)	Technical	SC-08(a)	Transmission Confidentiality & Integrity | Cryptographic or Alternate Physical Protection	SC-8 (1)	3.13.8						500.15											All Users	Basic
SC-9	Technical	SC-09	Transmission Confidentiality [withdrawn - incorporated in SC-08]																			N/A	N/A
SC-10	Technical	SC-10	Network Disconnect	SC-10	3.13.9		8-609					8.1.8	9.4.2, 11.2.8 & 13.1.1									Technical Users	Basic
SC-11	Technical	SC-11	Trusted Path																			Technical Users	Basic
SC-12	Technical	SC-12	Cryptographic Key Establishment & Management	SC-12	3.13.10							3.5, 3.5.1-3.5.3, 3.6 & 3.6.1-3.6.3	10.1.2									Technical Users	Basic
SC-12 (2)	Technical	SC-12(a)	Cryptographic Key Establishment & Management | Symmetric Keys	SC-12 (2)																		Technical Users	Enhanced
SC-12 (3)	Technical	SC-12(b)	Cryptographic Key Establishment & Management | Asymmetric Keys	SC-12 (3)																		Technical Users	Enhanced
N/A	Technical	SC-12(c)	Cryptographic Key Establishment & Management | Cryptographic Key Loss or Change									3.6.4 & 3.6.5										Technical Users	Basic
N/A	Technical	SC-12(d)	Cryptographic Key Establishment & Management | Control & Distribution of Cryptographic Keys									3.6.6-3.6.8										Technical Users	Basic
SC-13	Technical	SC-13	Use of Cryptography	SC-13	3.13.11		9-400					2.2.3 & 4.1	10.1.1, 14.1.2, 14.1.3 & 18.1.5	PR.DS-5		164.312(e)(2)(ii)						Technical Users	Basic
SC-14	Technical	SC-14	Public Access Protections																		All Users	Basic
SC-15	Technical	SC-15	Collaborative Computing Devices	SC-15	3.13.12								13.2.1								Technical Users	Basic
SC-16	Technical	SC-16	Transmission of Security Attributes				8-700														Technical Users	Enhanced
SC-17	Technical	SC-17	Public Key Infrastructure (PKI) Certificates	SC-17			8-303														Technical Users	Basic
SC-18	Technical	SC-18	Mobile Code	SC-18	3.13.13								12.2.1 &	DE.CM-5							Technical Users	Basic
SC-19	Technical	SC-19	Communications Technologies	SC-19	3.13.14		8-700														Management	Basic
SC-20	Technical	SC-20	Secure Name / Address Resolution Service (Authoritative Source)	SC-20									13.1.1								Technical Users	Basic
SC-21	Technical	SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	SC-21									13.1.1		8.6						Technical Users	Enhanced
SC-22	Technical	SC-22	Architecture and Provisioning for Name / Address Resolution Service	SC-22									13.1.1								Technical Users	Enhanced
SC-23	Technical	SC-23	Session Authenticity	SC-23	3.13.15		8-609														Technical Users	Enhanced
SC-24	Technical	SC-24	Fail in Known State				8-702														Technical Users	Enhanced
SC-25	Technical	SC-25	Thin Nodes				8-613														Technical Users	Enhanced
SC-26	Technical	SC-26	Honeypots																		Technical Users	Enhanced
SC-27	Technical	SC-27	Operating System-Independent Applications																		Technical Users	Basic
SC-28	Technical	SC-28	Encrypting Data at Rest	SC-28	3.13.16		8-604				500.15	3.4 & 3.4.1	8.2.3	PR.DS-1		164.312(a)(2)(iv)	17.04(5)	622(2)(d)(C)(iii)				Technical Users	Enhanced
SC-28 (1)	Technical	SC-28(a)	Encrypting Data at Rest | Cryptographic Protection	SC-28 (1)							500.15											Technical Users	Enhanced
SC-29	Technical	SC-29	Heterogeneity																			Technical Users	Enhanced
SC-29 (1)	Technical	SC-29(a)	Heterogeneity | Virtualization Techniques																			Technical Users	Basic
SC-30	Technical	SC-30	Concealment and Misdirection																			Technical Users	Enhanced
SC-31	Technical	SC-31	Covert Channel Analysis											PR.DS-5	12.10							Technical Users	Enhanced
SC-32	Technical	SC-32	Information System Partitioning																			Technical Users	Enhanced
SC-33	Technical	SC-33	Transmission Preparation Integrity [withdrawn - incorporated in SC-08]																			N/A	N/A
SC-34	Technical	SC-34	Non-Modifiable Executable Programs				8-302 8-304 8-311															Technical Users	Enhanced
SC-35	Technical	SC-35	Honeyclients																			Technical Users	Enhanced
SC-36	Technical	SC-36	Distributed Processing and Storage																			Technical Users	Enhanced
SC-37	Technical	SC-37	Out-of-Band Channels																			Technical Users	Enhanced
SC-38	Technical	SC-38	Operations Security																			Technical Users	Enhanced
SC-39	Technical	SC-39	Process Isolation	SC-39																		Technical Users	Enhanced
SC-39 (1)	Technical	SC-39(a)	Process Isolation | Hardware Separation																			Technical Users	Enhanced
SC-39 (2)	Technical	SC-39(b)	Process Isolation | Thread Separation																			Technical Users	Enhanced
SC-40	Technical	SC-40	Wireless Link Protection									11.1 & 11.1-11.1.2										Technical Users	Enhanced
SC-41	Technical	SC-41	Port and I/O Device Access																			Technical Users	Enhanced
SC-42	Technical	SC-42	Sensor Capability and Data										12.2.1									Technical Users	Enhanced
SC-43	Technical	SC-43	Usage Restrictions										9.4.2									Technical Users	Basic
SC-44	Technical	SC-44	Detonation Chambers										13.2.3	DE.CM-5								Technical Users	Basic
SI-1	Technical	SI-01	System and Information Integrity Policy & Procedures	SI-1			8-101	CC3.2	CC3.2				5.1.1, 5.1.2, 6.1.1, 12.1.1, 12.2.1, 18.1.1 & 18.2.2									Management	Basic

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
SI-2	Technical	SI-02	Flaw Remediation	SI-2	3.14.1 3.14.2 3.14.3	12	8-311 8-610	CC6.1	CC6.1			6.1 & 6.2	12.6.1 & 16.1.3	ID.RA-1 & PR.IP-12	4.5		17.04(6)	622(2)(d)(B)(iii)			5-1 5-2 5-3 5-4	Technical Users	Basic
SI-2 (1)	Technical	SI-02(a)	Flaw Remediation | Centralized Management			12						6.2, 6.4.5 & 6.4.5.1-6.4.5.4					17.04(7)				5-2	Technical Users	Basic
SI-2 (2)	Technical	SI-02(b)	Flaw Remediation | Automated Flaw Remediation Status	SI-2 (2)																		Technical Users	Enhanced
SI-2 (3)	Technical	SI-02(c)	Flaw Remediation | Time To Remediate Flaws / Benchmarks For Corrective Action	SI-2 (3)																	5-4	Technical Users	Enhanced
SI-3	Technical	SI-03	Malicious Code Protection (Malware)	SI-3	3.14.1 3.14.2 3.14.3 3.14.4 3.14.5	13	8-305	CC5.8	CC5.8			5.1, 5.1.1 & 5.2	12.2.1 & 14.1.2	DE.CM-4 & DE.DP-3	8.1 8.2 8.3 8.4 8.5	164.308(a)(5)(ii)(B)	17.04(7)				2-5 4-1 4-5	Technical Users	Basic
SI-3 (1)	Technical	SI-03(a)	Malicious Code Protection | Central Management	SI-3 (1)		13																Technical Users	Basic
SI-3 (2)	Technical	SI-03(b)	Malicious Code Protection | Automatic Updates	SI-3 (2)		13, 14						5.2									4-2	Technical Users	Basic
SI-3 (7)	Technical	SI-03(c)	Malicious Code Protection | Nonsignature-Based Detection	SI-3 (7)		13																Technical Users	Enhanced
N/A	Technical	SI-03(d)	Malicious Code Protection | Malware Protection Mechanism Testing			13																Technical Users	Basic
N/A	Technical	SI-03(e)	Malicious Code Protection | Evolving Malware Threats			13, 14															2-5 4-5	Technical Users	Basic
N/A	Technical	SI-03(f)	Malicious Code Protection | Always On Protection			13, 15						5.3									2-5 4-3 4-4	Technical Users	Basic
SI-4	Technical	SI-04	Information System Monitoring	SI-4	3.14.6 3.14.7		8-602					11.4	14.1.2, 12.4.1, 12.4.2, 12.4.3 & 12.7.1	ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-5, DE.CM-6, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1 & RS.CO-3	5.8 6.6 16.6 16.10	164.308(a)(1)(ii)(D) & 164.308(a)(5)(ii)(c)	17.03(2)(b)(3) & 17.04(4)				Technical Users	Basic
SI-4 (1)	Technical	SI-04(a)	Information System Monitoring | System-Wide Intrusion Detection System	SI-4 (1)																		Technical Users	Enhanced
SI-4 (2)	Technical	SI-04(b)	Information System Monitoring | Automated Tools for Real Time Analysis	SI-4 (2)								10.6, 10.6.1, 10.6.2 & 10.6.3										Technical Users	Enhanced
SI-4 (4)	Technical	SI-04(c)	Information System Monitoring | Inbound & Outbound Communications Traffic	SI-4 (4)	3.14.6																	Technical Users	Enhanced
SI-4 (5)	Technical	SI-04(d)	Information System Monitoring | System Generated Alerts	SI-4 (5)																		Technical Users	Enhanced
SI-4 (14)	Technical	SI-04(e)	Information System Monitoring | Wireless Intrusion Detection	SI-4 (14)								11.1										Technical Users	Enhanced
SI-4 (16)	Technical	SI-04(f)	Information System Monitoring | Correlate Monitoring Information	SI-4 (16)																		Technical Users	Enhanced
SI-4 (23)	Technical	SI-04(g)	Information System Monitoring | Host-Based Devices	SI-4 (23)																		Technical Users	Enhanced
SI-5	Technical	SI-05	Security Alerts, Advisories & Directives	SI-5	3.14.1 3.14.2 3.14.3		8-103						6.1.3, 6.1.4, 12.2.1, 14.1.2, 12.6.1 & 16.1.2	ID.RA-1, ID.RA-2, ID.RA-3 & RS.CO-5				622(2)(d)(B)(iii)				Technical Users	Basic
SI-6	Technical	SI-06	Security Functionality Verification	SI-6			8-613						12.4.1 & 12.4.4									Technical Users	Basic
SI-7	Technical	SI-07	Software & Information Integrity	SI-7			8-302					11.5 & 11.5.1	12.2.1, 14.1.2, 12.4.1 & 12.5.1	PR.DS-6								Technical Users	Enhanced
SI-7 (1)	Technical	SI-07(a)	Software & Information Integrity | Integrity Checks	SI-7 (1)				PI1.1	PI1.1													Technical Users	Enhanced
SI-7 (7)	Technical	SI-07(b)	Software & Information Integrity | Integration of Detection & Response	SI-7 (7)																		Technical Users	Enhanced
SI-8	Technical	SI-08	Spam Protection	SI-8			8-302															Technical Users	Basic
SI-8 (1)	Technical	SI-08(a)	Spam Protection | Central Management	SI-8 (1)																		Technical Users	Enhanced
SI-8 (2)	Technical	SI-08(b)	Spam Protection | Automatic Updates	SI-8 (2)																		Technical Users	Enhanced
SI-9	Technical	SI-09	Information Input Restrictions																			Technical Users	Enhanced
SI-10	Technical	SI-10	Information Input Validation	SI-10				PI1.2	PI1.2				8.2.3 & 14.1.2									Technical Users	Enhanced
SI-11	Technical	SI-11	Error Handling	SI-11																		Technical Users	Enhanced
SI-12	Technical	SI-12	Information Output Handling & Retention	SI-12				PI1.5 PI1.4	PI1.5 PI1.4		500.13	3.1 & 10.7	8.2.3, 18.1.3 & 18.1.4					622(2)(C)(i) & (iv)				Management	Basic
SI-13	Technical	SI-13	Predictable Failure Prevention															622(2)(d)(C)(iii)				Management	Basic
N/A	Technical	SI-13(a)	Predictable Failure Prevention | Computer Lifecycle Plan (CLP)																			Management	Basic
SI-14	Technical	SI-14	Non-Persistence																			Management	Basic

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
SI-15	Technical	SI-15	Information Output Filtering																			Technical Users	Enhanced
SI-16	Technical	SI-16	Memory Protection	SI-16																		Technical Users	Enhanced
SI-17	Technical	SI-17	Fail-Safe Procedures																			Management	Basic
AP-1	Privacy	AP-01	Authority To Collect							1.2.5 1.2.11 4.2.2												Management	Enhanced
AP-2	Privacy	AP-02	Purpose Specification					P2.1	P2.1	4.2.1												Management	Enhanced
AR-1	Privacy	AR-01	Governance & Privacy Program							1.1.0 1.1.2 1.2.1 1.2.2 1.2.8 1.2.9 1.2.11 2.1.0 4.2.3 8.2.1												Management	Basic
AR-2	Privacy	AR-02	Privacy Impact & Risk Assessment							1.2.4 4.2.3												Management	Enhanced
AR-3	Privacy	AR-03	Privacy Requirements For Contractors & Service Providers							4.2.3 7.2.4												Management	Enhanced
AR-4	Privacy	AR-04	Privacy Monitoring & Auditing					P6.5	P6.5	1.2.6 10.2.3 10.2.4 10.2.5												Management	Enhanced
AR-5	Privacy	AR-05	Privacy Awareness & Training					P1.2	P1.2	1.1.1 1.2.10												Management	Enhanced
AR-6	Privacy	AR-06	Privacy Reporting																			Management	Enhanced
AR-7	Privacy	AR-07	Privacy-Enhanced System Design & Development							6.2 7.2.2 7.2.3												Management	Enhanced
AR-8	Privacy	AR-08	Accounting of Disclosures																			Management	Enhanced
DI-1	Privacy	DI-01	Data Quality					P1.3 P7.1	P1 P7	9.2.1												Management	Enhanced
DI-2	Privacy	DI-02	Data Integrity							9.2.1												Management	Enhanced
DM-1	Privacy	DM-01	Minimization Of Personally Identifiable Information (PII)							4.1.2 9.2.1 9.2.2												Management	Enhanced
DM-2	Privacy	DM-02	Data Retention & Disposal					P3.1	P3.1	4.1.2 5.2.2 5.2.3	500.13											Management	Enhanced
N/A	Privacy	DM-02(a)	Data Retention & Disposal | Data Collection																			Management	Enhanced
N/A	Privacy	DM-02(b)	Data Retention & Disposal | Sensitive Data Storage									3.2 & 3.2.1-3.2.3										Management	Enhanced
N/A	Privacy	DM-02(c)	Data Retention & Disposal | Data Masking									3.3										Management	Enhanced
DM-3	Privacy	DM-03	Minimization Of Personally Identifiable Information (PII) In Testing, Training & Research							7.2.2 9.2.2												Management	Enhanced
IP-1	Privacy	IP-01	Consent							3.2.1 3.2.2 3.2.3 3.2.4												Management	Enhanced
IP-2	Privacy	IP-02	Individual Access					P3.2 P5.1 P6.8	P3.2 P5.1 P6.8	6.2.1 6.2.2 6.2.3 6.2.4 6.2.5 6.2.6												Management	Enhanced
IP-3	Privacy	IP-03	Redress					P5.2 P8.1	P5.2 P8.1	6.2.5 6.2.6 10.2.1 10.2.2												Management	Enhanced
IP-4	Privacy	IP-04	User Feedback Management					P5.2 P8.1	P5.2 P8.1	6.2.5 6.2.6 10.2.1 10.2.2												Management	Enhanced
SE-1	Privacy	SE-01	Inventory Of Personally Identifiable Information (PII)							7.2.2												Management	Enhanced

NIST 800-53 Rev 4	FIPS 199 Focus	WISP Standard #	Written Information Security Program - Standard Name	FedRAMP [MODERATE]	NIST 800-171 Rev1	FAR 52.204-21	NISPOM	AICPA SOC2 (2016)	AICPA SOC2 (2017)	AICPA / CICA GAPP	NY DFS	PCI DSS v3.2	ISO 27002:2013	NIST CSF	SANS Top 20 / CIS CSC v6.0	HIPAA	MA 201 CMR 17	OR 646A	FACTA	GLBA	UK Cyber Essentials	Target Audience	Applicability
SE-2	Privacy	SE-02	Privacy Incident Response					P6.3 P6.7	P6.3 P6.7	1.2.7 7.2.4												Management	Enhanced
TR-1	Privacy	TR-01	Privacy Notice					P1.1	P1.1	2.1.1 2.2.1 2.2.2 2.2.3 3.1.0 3.1.1 3.1.2 4.1.0 4.1.1 4.2.4 5.1.0 5.1.1 6.1.0 6.1.1 7.1.0 7.1.1 8.1.0 8.1.1 9.1.0 9.1.1 10.1.0 10.1.1												Management	Enhanced
TR-2	Privacy	TR-02	Safe Harbor							10.2.3												Management	Enhanced
TR-3	Privacy	TR-03	Dissemination of Privacy Program Information							2.1.1 3.1.0 4.1.0 4.1.1 6.1.0 6.1.1 7.1.0 7.1.1 8.1.0 8.1.1 9.1.0 9.1.1 10.1.0 10.1.1												Management	Enhanced
UL-1	Privacy	UL-01	Internal Use					P4.1	P4.1	5.2.1												Management	Basic
UL-2	Privacy	UL-02	Information Sharing With Third Parties							7.1.2 7.2.1 7.2.2 7.2.3												Management	Basic