WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	FAR 52.204-21	HIPAA	GLBA	NIST CSF v1.1	PCI DSS v3.2.1	US State MA 201 CMR 17.00	US State NY DFS	US State OR 646A	UK Cyber Essentials	UK Data Protection Act
1.0	Information Security Program Policy											
1.1	Management Direction for Information Security	5.1										
1.1.1	Policies for Information Security	5.1.1										
1.1.1.1	Publishing An Information Security Policy	5.1.1							500.03			
1.1.1.2	Information Security Program Plan			164.308(a)(1)(i) 164.316(a) 164.316(b)	6801(b)(1)	ID.GV-1 ID.GV-2	12.1 12.1.1	17.03(1), 17.04 & 17.03(2)(b)(2)	500.02			
1.1.1.3	Assigned Information Security Responsibilities			164.308(a)(2)	Safeguards Rule	ID.AM-6 ID.GV-2	12.5 12.5.1 12.5.2 12.5.3 12.5.4 12.5.5	17.03(2)(a)	500.04	622(2)(d)(A)(i)		
1.1.1.4	Information Security Resources											
1.1.1.5	Risk Management					ID.GV-4 ID.RM-1 ID.RM-2 ID.RM-3 PR.IP-7 PR.IP-8	12.2		500.09			
1.1.2	Review of Information Security Policies	5.1.2										
1.1.2.1	Information Security Documentation Review					PR.IP-7 PR.IP-8			500.03			
2	Information Security Organization Policy											
2.1	Internal Organization	6.1										
2.1.1	Information Security Roles & Responsibilities	6.1.1										
2.1.1.1	Roles & Responsibilities								500.04			
2.1.1.2	Position Categorization			164.308(a)(3)(i) 164.308(a)(3)(ii) 164.308(a)(3)(ii)(A)		PR.IP-11			500.04			
2.1.2	Segregation of Duties	6.1.2										
2.1.2.1	Incompatible Roles											
2.1.2.2	Two-Person Rule											
2.1.3	External Authorities	6.1.3										
2.1.3.1	Contacts With Authorities	6.1.3										
2.1.4	Special Interest Groups	6.1.4										
2.1.4.1	Contacts With Security Groups & Associations			164.308(A)(164.308(A)(5)(ii)(A)		ID.RA-2 RS.CO-5	5.1.2 6.1		500.10			
2.1.4.2	Security Industry Alerts & Notification Process			164.308(A)(5)(164.308(A)(5)(ii)(		RS.AN-5	6.2 12.4					
2.1.5	Information Security in Project Management	6.1.5										
2.1.5.1	Security Assessments					ID.GV-4 ID.SC-1 ID.SC-2 ID.SC-4 ID.RA-1 PR.IP-7 PR.IP-8 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)		
2.1.5.2	System Security Plan (SSP)					PR.IP-7 DE.DP-5						
2.2	Mobile Devices and Teleworking	6.2										
2.2.1	Mobile Device Management	6.2.1										
2.2.1.1	Access Control For Mobile Devices	6.2.1				PR.AC-3						
2.2.1.2	Central Management Of Mobile Devices											
2.2.1.3	Remote Purging											
2.2.1.4	Personally Owned Devices											
2.2.1.5	Tamper Protection & Detection											
2.2.2	Teleworking	6.2.2										
2.2.2.1	Telecommuting											
2.2.2.2	Remote Access	6.2.2				PR.AC-3 PR.PT-4	12.3.8 12.3.9					
2.2.2.3	Privileged Commands & Access											
2.2.2.4	Non-Local Maintenance					PR.MA-2						
2.2.2.5	Non-Local Maintenance Approvals & Notifications											
2.2.2.6	Non-Local Maintenance Cryptographic Protection						2.3					

WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	FAR 52.204-21	HIPAA	GLBA	NIST CSF v1.1	PCI DSS v3.2.1	US State MA 201 CMR 17.00	US State NY DFS	US State OR 646A	UK Cyber Essentials	UK Data Protection Act
2.2.2.7	Remote Disconnect Verification											
2.2.2.8	Auditing											
3	Human Resource Security Policy											
3.1	Prior to Employment	7.1										
3.1.1	Screening	7.1.1										
3.1.1.1	Personnel Screening			164.308(a)(3)(ii) 164.308(a)(3)(ii)(B)		PR.DS-5 PR.IP-11	12.7					
3.1.2	Terrms and Conditions of Employment	7.1.2										
3.1.2.1	Access Agreements			164.308(a)(4)(i)		PR.DS-5 PR.IP-11						
3.2	During Employment	7.2										
3.2.1	Management Responsibilities	7.2.1										
3.2.1.1	Rules of Behavior			164.310(b)			4.2 12.3 12.3.1 12.3.2 12.3.5 12.3.6 12.[illegible]0 12.4	17.03(2)(b)(2)				
3.2.1.2	Social Media & Social Networking Restrictions											
3.2.1.3	Position Categorization			164.308(a)(3)(i) 164.308(a)(3)(ii) 164.308(a)(3)(ii)(A)		PR.IP-11						
3.2.1.4	Third-Party Personnel Security					ID.AM ID.GV PR.[illegible] [illegible]-11						
3.2.2	Information Security Awareness, Education and Training	7.2.2										
3.2.2.1	Information Security Workforce					PR.AT-1 PR.AT-2 PR.AT-4 PR.AT-5						
3.2.2.2	Security Training					PR.AT-2 PR.AT-4 PR.AT-5	12.6.1 12.6.2	17.04(8)	500.14	622(2)(d)(A)(iv)		
3.2.2.3	Awareness Training for Sensitive Information						1.5 2.5 3.7 4.3 5.4 6.7 7.3 8.8 9.10 10.9 11.6 12.6 12.6.1 12.6.2 12.8.3 12.8.5 12.10.4		500.14			
3.2.2.4	Vendor Security Training											
3.2.2.5	Security Training Records						12.6.2					
3.2.2.6	Security Awareness			164.308(a)(5)(i) 164.308(a)(5)(ii)(A)		PR.AT-1	12.6	17.04(8) & 17.03(2)(b)(1)				
3.2.2.7	Testing, Training & Monitoring					PR.IP-10 DE.DP-1 DE.DP-2 DE.DP-3 DE.DP-5						
3.2.2.8	Practical Exercises											
3.2.2.9	Insider Threat Awareness											
3.2.2.10	Security Industry Alerts & Notification Process			164.308(A)(5)(ii) 164.308(A)(5)(ii)(A)		RS.AN-5	6.2 12.4					
3.2.3	Disciplinary Process	7.2.3										
3.2.3.1	Personnel Sanctions			164.308(a)(1)(ii)(C)		PR.IP-11		17.03(2)(d)				
3.2.3.2	Workplace Investigations											
3.3	Termination and Change of Employment	7.3										
3.3.1	Termination or Change of Employment Responsibilities											

WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	FAR 52.204-21	HIPAA	GLBA	NIST CSF v1.1	PCI DSS v3.2.1	US State MA 201 CMR 17.00	US State NY DFS	US State OR 646A	UK Cyber Essentials	UK Data Protection Act
3.3.1.1	Personnel Termination	7.3.1		164.308(a)(3)(ii) 164.308(a)(3)(ii)(C)		PR.IP-11	9.3	MA201CMR17 17.03(2)(e)				
3.3.1.2	High-Risk Terminations											
3.3.1.3	Personnel Transfer					PR.IP-11						
4	Asset Management Policy											
4.1	Responsibility for Assets	8.1										
4.1.1	Inventory of Assets											
4.1.1.1	Information System Inventory	8.1.1										
4.1.1.2	Information System Component Inventory						2.4					
4.1.1.3	Approved Deviations			164.310(d)(2)(iii)		ID.AM-1 ID.AM-2 PR.DS-3 PR.PT-3 DE.CM-7	1.1.2					
4.1.1.4	Network Diagrams					ID-AM-3	1.1.2 1.1.3					
4.1.2	Ownership of Assets	8.1.2										
4.1.2.1	Default Settings						2.5				1-1	
4.1.2.2	Shared Hosting Providers						2.6 A.1					
4.1.2.3	Intranets					ID.AM-4 PR.AC-3						
4.1.3	Acceptable Use of Assets	8.1.3										
4.1.3.1	Rules of Behavior			164.310(b)			4.2 12.3 12.3.1 12.3.2 12.3.5 12.3.6 12.3.10 12.4	17.03(2)(b)(2)				
4.1.3.2	Social Media & Social Networking Restrictions											
4.1.3.3	Acceptable Use for Critical Technologies						12.3 12.3.1 12.3.2 12.3.3 12.3.4 12.3.5 12.3.6 12.3.7 12.3.8 12.3.9 12.3.10					
4.1.4	Return of Assets	8.1.4										
4.1.4.1	Asset Collection											
4.2	Information Classification	8.2										
4.2.1	Classification of Information	8.2.1										
4.2.1.1	Security Categorization					ID.AM-5 ID.RA-4 ID.RA-5	9.6.1					
4.2.2	Labeling of Information	8.2.2										
4.2.2.1	Media Marking											
4.2.3	Handling of Assets	8.2.3										
4.2.3.1	Media Transportation			164.310(d)(1)		PR.PT-2	9.6 9.6.2 9.6.3 9.7	17.03(2)(c)		620		
4.2.3.2	Media Custodians											
4.2.3.3	Cryptographic Protection (Encrypting Data In Storage Media)								500.15			
4.3	Media Handling	8.3										
4.3.1	Management of Removable Media	8.3.1										
4.3.1.1	Media Use					PR.PT-2						
4.3.1.2	Media Access			164.308(a)(4)(ii)(C)		PR.PT-2						
4.3.2	Disposal of Media	8.3.2	52.204-21(b)(1)(vii)									
4.3.2.1	Data Retention & Disposal		52.204-21(b)(1)(vii)						500.13			Chapter29-Schedule1-Part1-Principle 5
4.3.2.2	Media Sanitization		52.204-21(b)(1)(vii)	164.310(d)(2)(i)		PR.DS-3 PR.IP-6	9.8 9.8.1 9.8.2		500.13	622(2)(d)(C)(i) & 622(2)(d)(C)(iv)		
4.3.2.3	Media Sanitization Documentation		52.204-21(b)(1)(vii)	164.310(d)(2)(ii)			9.7.1					
4.3.3	Physical Media Transfer	8.3.3										

WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	FAR 52.204-21	HIPAA	GLBA	NIST CSF v1.1	PCI DSS v3.2.1	US State MA 201 CMR 17.00	US State NY DFS	US State OR 646A	UK Cyber Essentials	UK Data Protection Act
4.3.3.1	Strict Control of Media						9.7 9.7.1					
5	Accesss Control Policy											
5.1	Business Requirements of Access Control	9.1										
5.1.1	Access Control	9.1.1	52.204-21(b)(1)(i) 52.204-21(b)(1)(v)								2-1 3-1	
5.1.1.1	Identification & Authentication					PR.AC-6	8.1		500.07		2-1	
5.1.1.2	Access To Sensitive Data						7.1 7.1.1 7.1.2 7.1.3 7.1.4					
5.1.1.3	Access Control Procedures			164.312(a)(1)			8.1 8.4					
5.1.2	Access to Networks and Network Services	9.1.2	52.204-21(b)(1)(ii)									
5.1.2.1	Least Functionality					PR.IP-1	1.1.5 1.2.1 2.2.2 2.2.4 2.2.5	17.03(2)(a)			2-1	
5.1.2.2	Prevent Program Execution											
5.2	User Access Management	9.2	52.204-21(b)(1)(i)								3-7	
5.2.1	User Registration and De-Registration	9.2.1										
5.2.1.1	User ID Management						8.1 8.1.1 8.1.2 8.1.3 8.1.4 8.1.5 8.1.6 8.1.7 8.1.8				3-6	
5.2.1.2	Account Management			164.312(d)		PR.AC-1 PR.AC-4 PR.AC-6 DE.CM-1 DE.CM-3	8.1.3 8.1.4 8.1.5 8.2.2 8.5 8.5.1 8.6 8.7	17.04(1(a)			3-1	
5.2.2	User Access Provisioning	9.2.2	52.204-21(b)(1)(i)								3-1	
5.2.2.1	Account Provisioning					PR.AC-6	8.2 8.2.1 8.2.2 8.2.3 8.2.4 8.2.5 8.2.6				3-1	
5.2.2.2	Role-Based Access Control (RBAC)			164.308(a)(4(ii)(A) 164.308(a)(4(ii)(B) 164.308(a)(4(ii)(C)			7.1 7.1.1 7.1.2 7.1.3 7.1.4 7.2 7.2.1 7.2.1 7.2.3				3-1	
5.2.3	Management of Privileged Access Rights	9.2.3	52.204-21(b)(1)(i)								3-2	
5.2.3.1	Privileged Commands & Access										3-2 3-3 3-4 3-5	
5.2.4	Management of Secret Authentication Information of Users	9.2.4										
5.2.4.1	User Identification & Authentication for Organizational Users			17.04(1)(c) 17.04(2)(b)		PR.AC-7	8.1.1 8.2					
5.2.4.2	Multifactor Authentication		52.204-21(b)(1)(vi)			PR.AC-7	8.3 8.3.1 8.3.2		500.12			
5.2.4.3	Identifier Management (User Names)		52.204-21(b)(1)(vi)	164.312(a)(2)(i)				17.04(1)(d)				
5.2.4.4	Privileged Account Management		52.204-21(b)(1)(vi)									
5.2.4.5	Identification & Authentication (Non-Organizational Users)		52.204-21(b)(1)(vi)									
5.2.4.6	Service Provider Identification & Authentication (Vendors)		52.204-21(b)(1)(vi)									

WISP #	Written Information Security Program (WISP) Section	ISO 27002:2013	FAR 52.204-21	HIPAA	GLBA	NIST CSF v1.1	PCI DSS v3.2.1	US State MA 201 CMR 17.00	US State NY DFS	US State OR 646A	UK Cyber Essentials	UK Data Protection Act
5.2.5	Review of User Access Rights	9.2.5										
5.2.5.1	Periodic Review											
5.2.6	Removal or Adjustment of Access Rights	9.2.6	52.204-21(b)(1)(i)									
5.2.6.1	Access Enforcement			164.308(a)(4)(i) 164.308(a)(4)(ii)		PR.AM-3 PR.AC-4 PR.PT-3	7.1 7.1.1 7.1.2 7.1.3 7.1.4 7.2 7.2.1 7.2.3	17.04(1)(b) & 17.04(2)(a)		622(2)(d)(C)(iii)		
5.3	User Responsibilities	9.3										
5.3.1	Use of Secret Authentication Information	9.3.1										
5.3.1.1	Individual Credentials						8.6					
5.3.1.2	Credential Sharing						8.5 8.5.1					
5.4	System and Application Access Control	9.4	52.204-21(b)(1)(v)									
5.4.1	Information Access Restriction	9.4.1	52.204-21(b)(1)(ii)									
5.4.1.1	Access Control Lists (ACLs)						7.2 7.2.1 7.2.3					
5.4.1.2	Database Access						8.7					
5.4.2	Secure Log-On Procedures	9.4.2	52.204-21(b)(1)(vi)									
5.4.2.1	Trusted Communications Path											
5.4.2.2	Device-To-Device Identification & Authentication											
5.4.2.3	System Use Notification (Logon Banners)											
5.4.2.3.1	System Use Notification | Standardized Microsoft Windows Logon Banner											
5.4.2.3.2	System Use Notification | Truncated Logon Banner											
5.4.2.4	Previous Logon Notification											
5.4.3	Password Management System	9.4.3	52.204-21(b)(1)(i)									
5.4.3.1	Authenticator Management (Passwords)			164.308(a)(5)(ii)(D)			8.1.2 8.2.3 8.2.4 8.2.5	17.04(1)(b)-(e) & 17.04(2)(b)				
5.4.3.2	Vendor-Supplied Defaults						2.1 2.1.1 8.3				2-1 2-2	
5.4.3.3	Authenticator Feedback											
5.4.3.4	Cryptographic Module Authentication						8.2.1					
5.4.3.5	Re-Authentication						8.1.8					
5.4.4	Use of Privileged Utility Programs	9.4.4	52.204-21(b)(1)									
5.4.4.1	Access Enforcement			164.308(a)(4)(i) 164.308(a)(4)(ii)		PR.AM-3 PR.AC-4 PR.PT-3	7.1 7.1.1 7.1.2 7.1.3 7.1.4 7.2 7.2.1 7.2.3	17.04(1)(b) & 17.04(2)(a)		622(2)(d)(C)(iii)		
5.4.4.2	Least Privilege					PR.AC-4 PR.DS-5				622(2)(d)(C)(iii)		
5.4.5	Access Control to Program Source Code	9.4.5										
5.4.5.1	Source Code											
5.4.5.2	Library Privileges											
6	Cryptography Policy											
6.1	Cyrptographic Controls	10.1										
6.1.1	Use of Cryptographic Controls	10.1.1							500.15			
6.1.1.1	Use of Cryptography			164.312(e)(2)(ii)		PR.DS-5	2.2.3 4.1		500.15			
6.1.1.2	Transmission Confidentiality			164.312(e)(1) 164.312(e)(2)(i)				17.04(3)		622(2)(d)(C)(iii)		
6.1.1.3	Non-Local Maintenance Cryptographic Protection						2.3					
6.1.1.4	Wireless Access Authentication & Encryption						4.1.1		500.15			
6.1.1.5	Encrypting Data At Rest			164.312(a)(2)(iv)		PR.DS-1	3.4 3.4.1	17.04(5)	500.15	622(2)(d)(C)(iii)		
6.1.1.6	Non-Console Administrative Access						2.3					
6.1.2	Key management	10.1.2										