CURRENT ADHICS STATUS

Section Name	Domain Name	Sub Domains	Action Plan Required	Required Documents
Section A	Governance	**High End Policy**	Highend Policy Required Periodic reviews and audits of policy compliance by the InfoSec Team.	ADHICS V2 and Previous Highend Policy Policy review Checklist
		Governance Structure Policy	Ensure the HIIP Workgroup is led by a Chief Information Security Officer (CISO) and includes representatives from various business and support functions. Verify that the policy is periodically reviewed and updated to account for evolving security threats and changes in regulations	Policy with Updated governance
		ISGC minutes of Meeting docs for 2 quarters	Need to Prepare MoM for last 2 quarters	MoM Required
		RHHCS Organization Chart	IT will share the Chart with Quality	Organization Chart
	Asset Classification	Evidence	Need to be updated for 2025	Asset Register/ Criticality Assessment
			Need to be updated for 2025	Asset Sticker (Classification Lable and Asset Number)
			Need to be updated for 2025	Confidentiality sticker for files
			Need to be updated for 2025	Asset Classification Tracker
			Need to be updated for 2025	Asset Policy
	Vision Mission and Values	Related Documents	same shall be used	Mission and Vision documents
	Risk Management	Periodic Assesement	same shall be used	Risk Management Policy
			revise the document	Risk Register
			revise the document	Risk Assesment
		Implementation	revise the document	Risk Treatement Action Plan
			revise the document	Risk Treatement Action Status
			revise the document	Risk Register
			revise the document	Risk Management Policy
		Periodic Management	revise the document	Risk Management Policy
			revise the document	Risk Assesment
				Controlled Document Tracker
			revise the document	Management Annual Activity Schedule & Improvement Initiatives
	Control & Compliance Audit	Compliance	Revised the document to current date	Compliance Tracker/Legal Register
		Audits & Assesment		Information Security Internal Audit Plan
				Internal Audit Reports and Action Tracker
			Revised the document to current date	Legal Register
			Same Policy to be used	Policy
			evidence needs to be added by HR and must be validated by IT	Disciplinary Process
			evidence needs to be added by HR and must be validated by IT	MOI
			evidence needs to be added by HR and must be validated by IT	Employees-Non Disclosure Agreement

			•	
		HR1 and 1.1 Security Policy	evidence needs to be added by HR and must be validated by IT	Background Verification
			evidence needs to be added by IT	Training & Awareness
			evidence needs to be added by HR and must be validated by IT	Contractors /Third Party - NDA
			evidence needs to be added by HR and must be validated by IT	Contractors / Third Party Policy Acknowledgemnt
		HR 2 Prior to Employment	evidence needs to be added by HR and must be validated by IT	2.1 Background Verification for IT & Clinical
			evidence needs to be added by HR and must be validated by IT	2. 2 Job Description for IT & Clinical
			evidence needs to be added by HR and must be validated by IT	2.1 Non Disclosure Agreement for IT & Clinical
			evidence needs to be added by HR and must be validated by IT	2.1 Clinic soft Training Test Attendance feedback form and Training Certificate
			evidence needs to be added by HR and must be validated by IT	2.1Orientation Attendance & Undertaking acknowledgement
		HR 3 During Employment	evidence needs to be added by HR and must be validated by IT	3.1 ,3.2 Orientation Attendance & Undertaking acknowledgement
			evidence needs to be added by HR and must be validated by IT	3.1,3.2 E-learning Policies & Procedures Acknowledgement form
			evidence needs to be added by HR and must be validated by IT	3.1 Code of Ethics
			evidence needs to be added by IT	3.4 Cyber Security drill and simulating phishing attacks
			evidence needs to be added by HR and must be validated by IT	3.3 Disciplinary Process
			evidence needs to be added by IT	3.4 Awareness Posters
			evidence needs to be added by HR and must be validated by IT	3.4 HR Circular for Cyber security Awareness
			evidence needs to be added by HR and must be validated by IT	3.1 Employee signed NDA
			evidence needs to be added by HR and must be validated by IT	3.1 Employee non circum agreement
				Leavers List
			evidence needs to be added by HR and must be validated by IT	3.5 Third Party Policy Acknowledgement & NDA
			evidence needs to be added by HR and must be validated by IT	4.1, 4.3 Email Deactivation Screenshot from HR Email
			evidence needs to be added by HR and must be validated by IT	4.1,4.3 Email Deactivation Screenshot from Cpanel
			evidence needs to be added by IT	4.1 IT acknowledgement to HR email screenshot
			evidence needs to be added by HR and must be validated by IT	4.1 , 4.2, 4.3 Asset Clearance Form and Asset return

			•	
	HR	HR 4 Termination or Clearance	evidence needs to be added by HR and must be validated by IT	4.1,4.3 Licence Cancellation Request
			evidence needs to be added by HR and must be validated by IT	4.2 Leave Endorsement Signed
			evidence needs to be added by HR and must be validated by IT	4.4 Department Clearance
			evidence needs to be added by HR and must be validated by IT	4.4 Duty Handover
			evidence needs to be added by HR and must be validated by IT	4.4 Exit Endorsement
			evidence needs to be added by HR and must be validated by IT	4.4 Internal Transfer or Change of role request form
		AM 1 AM Policy	same policy can be used	AM 1.1 Policy
			evidence needs to be added by IT	AM 1.1Asset Register
			evidence needs to be added by IT	AM 1.1 Asset Disposal Procedure
			evidence needs to be added by IT	AM 1.1 IT Asset List for RHHCS
			evidence needs to be added by IT	AM 1.2 Allocation of Medical Assets [B] [S] These additional controls specific to medical devices and equipment are to be taken into account when developing the asset management policy mandated by AM 1.1. Medical equipment and devices play a crucial role in the treatment and diagnosis of illness and disease. However, as discussed elsewhere in this document, they also introduce new risks. This control is intended to help manage the risk associated with the use of medical equipment and devices. Specific attention to access control, authentication, authorization, handling procedures, risk log and disposal of medical equipment and devices is required as part of this control. This can be included as part of the asset management policy, in a single policy document, or can be represented by a separate policy reflecting the complex nature of certain entities.
			evidence needs to be added by IT	AM1.1 Bio-Medical Asset List for RHHCS
			evidence needs to be added by IT	AM 2.1 IT Asset List for RHHCS
			evidence needs to be added by IT	AM 2.2 Asset Relationship [A] The inventory should establish the relations between various types of information assets, in support of care delivery. Sample illustration: Service A => needs B Information => supplied by C Device/Equipment/Process/Dependent-Service => processed using D Application (ERP/EMR/Office Automation Applications/etc.) => running on E Technology (server/systems) => supported/operated/managed by XYZ Roles (human resources involved in care delivery)

		AM 2 Management of Assets	evidence needs to be added by IT	Bio-Medical Asset List for RHHCS AM 2.3 Asset Ownership [B] Every identified asset should be assigned an ‘Owner’. The owner maybe an individual or a designated role. The purpose is to assign responsibility for the security of the asset. The responsibility of the ‘Owner’ should be to: a) Define/identify the control requirements to minimize the impact of risk, due to the compromise of assets under his/her ownership. b) Review the adequacy of implemented control measures periodically and amend/modify the control environment as necessary. c) Ensure effectiveness of the implemented controls, in addressing the risk environment. d) Authorize access and/or use of information assets. e) Define and periodically review access restrictions and classifications, in line with the access control policy of the entity. Note that the patient is the final owner of his/her personal healthcare information and ‘Owner’ designated by the entity acts on behalf him/her. Ownership of shared IT resources (email system, Active Directory, Common File Server, etc.) should be collectively owned by the entity’s Information Technology/System or Information and Communication Technology Function.
			evidence needs to be added by IT	AM 2.4 Whitelisted Applications
		AM 3 Asset Classification and Labelling	evidence needs to be added by IT	AM 3.1 Policy
			evidence needs to be added by IT	AM 3.1 Bio-Medical Asset List for RHHCS
			evidence needs to be added by IT	AM 3.2 Bio-medical and IT asset
			evidence needs to be added by IT	AM 3.3 IT Asset List for Reyada
			evidence needs to be added by IT	AM 3.4 Change Request form
			evidence needs to be added by IT	AM 3.5 Asset Management Policy
			evidence needs to be added by IT	AM 3.7 Policy
			evidence needs to be added by IT	AM 3.7 Asset List
			evidence needs to be added by IT	AM 3.7 Biomedical Device
			evidence needs to be added by IT	AM 3.7 Network Diagram for RHHCS
			evidence needs to be added by IT	AM 4.1 Policy
			evidence needs to be added by IT	AM 4.2 Policy

			•	
		AM 4 Asset Handling	evidence needs to be added by IT	AM 4.3 Removable Media Block from Server (Group Policy Management Screenshot) AM 4.3 Access Allocation for Medical Devices [B] [S] Access and privilege allocation for medical devices should be provided to defined roles, with essential qualification and experience required to operate. Medical equipment and devices should be protected from unauthorized operation. Where available, access should be restricted with passwords following the entity password policy. The entity should: a) Secure and safe-guard medical devices and equipment in accordance with its classification scheme and risk factor.
			evidence needs to be added by IT	AM 4.4 Removable Media Block from Server (Group Policy Management Permissions Screenshot) AM 4.4 Security of Information within Medical Devices [T] [S] The Medical devices and equipment often collect and process sensitive Health Information. The entity should prevent unauthorized disclosure, modification, destruction or loss of patient healthcare information stored on medical devices and equipment. While security measures such as encryption are essential to guard against hackers, entity must also ensure that Health Information is not lost or stolen tHRough employee's neglect or malicious intent.
			evidence needs to be added by IT	AM 4.5 Bio-Medical Asset List for RHHCS & Manuals AM 4.5 Communication Facility for Medical Devices [T] Healthcare facilities should consider wired communication facility for medical devices and equipment. Usage of wireless communication facility with medical devices and equipment should be avoided to the extent possible. Use of wireless networking introduces the possibility of Denial of Service (DoS) attacks as well as Man in the Middle (MitM) attacks which can affect the availability and confidentiality of data on the internal network. This is especially critical for medical devices and equipment. See also CM 5.4. If wireless networks are used, then the strongest available authentication and encryption should be used. Connections should be logged, monitored, and restricted to trusted devices.
			evidence needs to be added by IT	AM 4.6 IT Asset List for RHHCS & Bio-Medical Asset List for RHHCS
			evidence needs to be added by IT	AM 4.7 NDA for vision
			evidence needs to be added by IT	AM 4.8 Not Applicable (No wireless media for Bio Medical devices)
			evidence needs to be added by IT	AM 4.9 Antivirus Status Screenshot For Server & System & Tabletes
			evidence needs to be added by IT	AM 4.10 RHHCS Asset Movement form

	Asset Management	AM 5 Asset Disposal	evidence needs to be added by IT	AM 5.1 Asset Disposal Procedure & Asset Disposal Form & Patient MR retention and Disposal Policy & IT Asset Disposal Policy & IT equipment disposal form & IT asset disposal life cycle inventory record & checklist for Pre IT disposal
			evidence needs to be added by IT	AM 5.2 Patient MR retention and Disposal Policy & IT Asset Disposal Policy & IT equipment disposal form & IT asset disposal life cycle inventory record & checklist for Pre IT disposal
			evidence needs to be added by IT	AM 5.3 Asset Disposal Procedure & Asset Disposal Form & Patient MR retention and Disposal Policy & IT Asset Disposal Policy & IT equipment disposal form & IT asset disposal life cycle inventory record & checklist for Pre IT disposal &
			evidence needs to be added by IT	AM 5.4 IT Asset Disposal Policy & IT Equipment disposal form & IT asset disposal life cycle inventory record & Checklist for Pre IT Disposal
			evidence needs to be added by IT	AM 5.5 Asset Disposal Procedure & Asset Disposal Form & Patient MR retention and Disposal Policy & IT Asset Disposal Policy & IT equipment disposal form & IT asset disposal life cycle inventory record & checklist for Pre IT disposal
			evidence needs to be added by IT	AM 5.6 Asset Disposal Procedure & Asset Disposal Form & IT Asset Disposal Policy & IT equipment disposal form & IT asset disposal life cycle inventory record & checklist for Pre IT disposal
			evidence needs to be added by IT	AM 5.7 Asset Disposal Procedure & Asset Disposal Form & IT Asset Disposal Policy & IT equipment disposal form & IT asset disposal life cycle inventory record & checklist for Pre IT disposal
		PE ADMCC	NA	CCTV service Report
			NA	Maintanance Checklist
			Send email to ADMCC and get it documented that we are not eligible for MCC	MCC Certificate
			NA	Police Checklist
			NA	SAD Certificate
			CCTV log sheet from Raja	CCTV Access Record
		PE 1 Security Policy	evidence needs to be added by IT	PE1.1 PE Policy
			evidence needs to be added by IT	PE1.2 PE Policy
			evidence needs to be added by IT	List of Bio Medical Asset List
			evidence needs to be added by IT	PE 2.1 PE Policy
			evidence needs to be added by IT	PE 2.2 Advanced
			evidence needs to be added by IT	PE 2.3vision EMR Log History Screenshot & Secure Area access & List of Secure Areas & secure Area Access form

	Physical & Environmental Security	PE 2 Secure Area	evidence needs to be added by IT	PE 2.4 RHHCS clinic Secure Area & Logs CCTV & Server & Secure Area access form
			evidence needs to be added by IT	PE 2.5 Secure Area & Secure Area access form Physical Access review -Bi Annually
			evidence needs to be added by IT	PE 2.6 UPS Photo
			evidence needs to be added by IT	PE 2.7 Risk Register
			evidence needs to be added by IT	PE 2.8 Radiation Sticker Photo in both X-Ray Rooms
			evidence needs to be added by IT	PE 2.9 NDA Agreement for CCTV CCTV-ADMCC-Not Applicable- Confirmaion mail
			evidence needs to be added by IT	PE 2.10 Policy
		PE 3 Equipment Security	evidence needs to be added by IT	PE 3.1 Fire Extinguisher PPM report & Fire Extinguisher vendor access record & Risk Register & PE Policy. Fire and safety training record with certification. Fire Drill Report
			evidence needs to be added by IT	PE 3.2 UPS Photo PPM maintainence -Physical Security System
			evidence needs to be added by IT	PE 3.3 Not applicable
			evidence needs to be added by IT	PE 3.4 Server room cable arrangment Photo,Server room temperature
			evidence needs to be added by IT	PE 3.5 Not applicable
			evidence needs to be added by IT	PE 3.6 Acceptable usage Policy (all the user should read in Elearning) & Session Time GPO desktop & server screenshot
			evidence needs to be added by IT	PE 3.7 Clear desk & Clear Screen Policy
		AC1 Access control Policy	evidence needs to be added by IT	AC 1.1 Access Control Policy
		AC 2 User Access Management	evidence needs to be added by IT	AC 2.1 Access Control Policy
			evidence needs to be added by IT	AC 2.2 Not Applicable
			evidence needs to be added by IT	AC 2.3 Firewall Password Lock out session Screenshot & Password Security Policy & Server Lock out Policy Screenshot
		AC 3 Equipment & Devices Access control	evidence needs to be added by IT	AC 3.1 Removable block screenshot
			evidence needs to be added by IT	AC 3.2 Not Applicable (Tele working sites)
		AC 4 Access Review	evidence needs to be added by IT	AC 4.1 Access Review report Signed & Vision Privilage form
			evidence needs to be added by IT	AC 5.1 Access Review report Signed
			evidence needs to be added by IT	AC 5.2 Remote Authentication (Quick Assist with system Information Screenshot)

			•	
	Access Control	AC 5 NAC	evidence needs to be added by IT	AC 5.3 RHHCS IT Asset List AC 5.3 Remote Diagnostic and Configuration Protection [A] The entity should control access to all information assets for the purpose of diagnostic and configuration. Medical equipment, computer systems, network systems, applications, communication systems etc. may have a remote diagnostic and configuration port for use by maintenance engineers. If unprotected, these diagnostic ports provide a means of unauthorized access. Connectivity to these ports should be enabled only when required and with authorization. Processes are created to regulate logical and physical access to the port, such as ensuring that diagnostic and configuration ports are only available by to authorized hardware/software support people The entity should: a) Identify and whitelist all ports, services and utilities that are used for troubleshooting, and for diagnostics and configuration purposes. b) Provides rationale or define security controls for the diagnostic and configuration services and utilities that are essential, and disable services and utilities that are not required. c) Restrict access for remote troubleshooting, diagnostic and configuration to authorized roles and from authorized workstations.
			evidence needs to be added by IT	AC 5.4 Not Applicable
			evidence needs to be added by IT	AC 5.5 Firewall interface screenshot & Policy Screenshot & Network Diagram
			evidence needs to be added by IT	AC 5.6 Firewall interface screenshot & Policy Screenshot & Network Diagram
			evidence needs to be added by IT	AC 5.7 Wi-FI SSID Broadcast screenshot (Aruba AP Screenshot)
			evidence needs to be added by IT	Ports in firewall need to whitelist all other port need to block
		AC 6 Operating System Access Control	evidence needs to be added by IT	AC 6.1 Server GPO screenshot & Post Log Banner in Firewall & Pre login Banner in Firewall
			evidence needs to be added by IT	AC 6.2 EMR Users active & Inactive users & Firewall local traffic screenshot
			evidence needs to be added by IT	AC 6.3 Not Appliocable
		AC 7 Application & info Access control	evidence needs to be added by IT	AC 7.1 Logs CCTV & server
			evidence needs to be added by IT	AC 7.2 RHHCS Secure Areas
			evidence needs to be added by IT	AC 7.3 All vendors NDA (Bio Medical & IT) Vision
		OM 1 Operation Management Policy	evidence needs to be added by IT	Operation Management Policy
			evidence needs to be added by IT	OM 2.1 RHHCS Baseline Configuration
			evidence needs to be added by IT	OM 2.2 Bios Medical Manuals

		OM 2 Operational Procedures	evidence needs to be added by IT	OM 2.3 Change Management Policy & Updated Change Request form & change Management logs & Change Impact assesment Change Proposal for EMR migration Change Management process
			evidence needs to be added by IT	OM 2.4 Change Management Policy & Change Request form & change Management logs & Change Impact assesment Change Proposal for EMR migration Change Management process & EMR Roles (Approved privilage Document & Insta application role screenshot)
			evidence needs to be added by IT	OM 2.6 Not Applicable
			evidence needs to be added by IT	OM 3.1 Not Applicable
		OM 3 Planning & Acceptance	evidence needs to be added by IT	OM 3.2 Not Applicable
			evidence needs to be added by IT	System Acceptance Tracker
		OM 4 Malware Protection	evidence needs to be added by IT	OM 4.1 AV desktop & AV Server
			evidence needs to be added by IT	OM 4.2 Not Applicable
		OM 5 Backup & Archival	evidence needs to be added by IT	Antivirus for Installation / Periodic Scans
			evidence needs to be added by IT	OM 6.1 Not Applicable
			evidence needs to be added by IT	OM 6.2 Not Applicable
			evidence needs to be added by IT	OM 6.3 Firewall Policy Screenshot & Web filtering Screenshot
			evidence needs to be added by IT	OM 6.4 Clock Sync Screenshot
			evidence needs to be added by IT	OM 6.5 RHHCS Patch Management Policy & Server Patch History Screenshot

			•	
			evidence needs to be added by IT	Patch Management 6.6 Patch Management Procedure [B] [S] The entity should define and establish formal procedure for updating and patching of information system and application, medical devices and equipment. Vulnerabilities are regularly identified in any hardware or software with network connectivity. These vulnerabilities are then patched with software updates and/or firmware updates. Patches are given tHRee levels of criticality. Depending on the criticality a deadline for rollout should be defined. Testing of patches on a small subset is recommended. 212 The entity should: a) Restrict the usage of obsolete software/technology/medical devices/ equipment b) Ensure all systems and devices that process or communicate information are timely patched and protected c) Define criteria and process for application of standard, urgent and critical patches d) Ensure all critical security patches are applied as soon as practicable from the date of release. e) Ensure patches are deployed to a subset of systems or devices to allow testing before deployment to all. f) Ensure firmware on devices are kept updated g) Ensure third parties provide advance notification to entity prior to the release of any patches or updates to the offered product or service h) Periodically validate patch status of systems and devices in use i) Ensure security patches and updates are obtained from trusted sources and are periodically implemented
			evidence needs to be added by IT	Tracking of Patches [A] 6.6 The entity should have mechanisms in place for effective tracking of patches to: a) Ensure software and systems are up-to-date with the latest security patches. By tracking and installing security patches in a timely manner, entity can reduce the risk of your system being compromised b) Install software updates and patches that sometimes cause compatibility issues with other software or hardware c) Identify areas of inefficiency and make improvements to streamline the process. This can save time and resources and help ensure that patches are deployed in a timely and effective manner. Automated patch management systems are recommended for larger organizations, dependent on their risk environment
		OM 6 Monitoring Logging	evidence needs to be added by IT	Logging & Monitoring Tracker

			•	
	Operations Management	OM 7 Security Assessment and Vulnerability Mgmt	evidence needs to be added by IT	OM 7.1 vision VAPT report
			evidence needs to be added by IT	OM 7.2 All NDA agreement & third Party Agreement Signed & contract acknowledgement receipts
	Communications	CM 1 Communication Policy	evidence needs to be added by IT	CM1.1 Policy
		CM 2 Information Exchange	evidence needs to be added by IT	CM 2.1 Electronic communication usage policy & Health Information and Security Policy
			evidence needs to be added by IT	CM 2.2 Email creation Mail screenshot from HR and Reply mail Screenshot
			evidence needs to be added by IT	CM 2.3 Email Password Sharing Evidence Screenshot
			evidence needs to be added by IT	CM 2.4 NDA agreement for vision
			evidence needs to be added by IT	CM 2.5 vision Agreement ,NDA & Bio Medical vendors Agreement & NDA
			evidence needs to be added by IT	CM 2.6 Malaffi Connected user Email screenshot and Excel
			evidence needs to be added by IT	CM 2.7 Email Disclaimer English & Arabic
			evidence needs to be added by IT	CM 2.8 Not Applicable
		CM 3 Electronic Commerce	evidence needs to be added by IT	CM 3.1 Not applicable
			evidence needs to be added by IT	CM 3.2 Not Applicable
			evidence needs to be added by IT	CM 3.3 Advanced
		CM 4 Information Sharing Platforms	evidence needs to be added by IT	CM 4.1 Advanced
			evidence needs to be added by IT	CM 4.2 Web and Email hosting geographical location
			evidence needs to be added by IT	CM 4.3 NDA Agreement vision & bio Medical Vendor
		CM 5 Network Security Management	evidence needs to be added by IT	CM 5.1 Network Diagram
			evidence needs to be added by IT	CM 5.2 SSID Broadcast
			evidence needs to be added by IT	CM 5.3 SSID Broadcast
			evidence needs to be added by IT	CM 5.4 SSID Broadcast
	Health Information & Security	HI 1 Protection Policy	evidence needs to be added by IT	HI 1.1 Policy
		HI 2 Policy Needs to be validated	evidence needs to be added by IT	HI 2 Policy
	Third Party	TP 1 Security Policy	evidence needs to be added by IT	TP 1.1 Policy (vision, Bio Medical Vendors all document)
		TP 2 Third Party Service Delivery & Monitoring	evidence needs to be added by IT	TP 2.1 SLA Agreement (vision)
			evidence needs to be added by IT	TP 2.2 RHHCS Service Report (Bio Medical Vendor)
			evidence needs to be added by IT	TP 2.3 Vendors Contract
		SA 1 Policy	evidence needs to be added by IT	SA 1.1 Information System AcquisaTtion Policy & Cryptographic Policy
		SA 2 Security	evidence needs to be added by IT	SA 2.1 Not Applicable
			evidence needs to be added by IT	SA 2.2 Not Applicable
		SA 3 Correction	evidence needs to be added by IT	SA 3.1 Not Applicable
			evidence needs to be added by IT	SA 3.2 Not Applicable
			evidence needs to be added by IT	SA 3.3 Vision Login Page Screenshot
			evidence needs to be added by IT	SA 3.4 Not Applicable
			evidence needs to be added by IT	SA 3.5 Not Applicable
		SA 4 Cryptography	evidence needs to be added by IT	SA 4.1 Cryptography Policy

		●		
	Information System Acquisition development and Maintenance	SA 5 System Files	evidence needs to be added by IT	SA 5.1 Advanced
			evidence needs to be added by IT	SA 5.2 Backup Test Restoration report
			evidence needs to be added by IT	SA 5.3 Not Applicable
		SA 6 Software	evidence needs to be added by IT	SA 6.1 Vision Agreement
		SA 7 SCM	evidence needs to be added by IT	SA 7.1 NDA & AMC Documents
			evidence needs to be added by IT	SA 7.2 Advanced
			evidence needs to be added by IT	SA 7.3 Advanced
			evidence needs to be added by IT	SA 7.4 Advanced
			evidence needs to be added by IT	SA 7.5 Advanced
			evidence needs to be added by IT	SA 7.6 Advanced
			evidence needs to be added by IT	SA 7.7 Advanced
	Incident Management	IM 1 Information Security Incident Policy	evidence needs to be added by IT	IM 1.1 Information Security Incident Management Procedures & IT checklist for Incident register and Metication
		IM 2 Incident Management & Improvements	evidence needs to be added by IT	IM 2.1 Cyber Security common causes of data breach & Awareness Circular & Desk notice for Awareness Phising Training & drilling
			evidence needs to be added by IT	IM 2.2 IT incident report Screenshot
			evidence needs to be added by IT	IM 2.3 IM Policy
			evidence needs to be added by IT	IM 2.4 Cyber Security common causes of data breach & Awareness Circular & Desk notice for Awareness Phising Training & drilling & orientation attendance & Incident Management form signed evidence
			evidence needs to be added by IT	IM 2.5 IT Incident Management form
			evidence needs to be added by IT	IM 2.6 Advanced
		IM 3 Information Security Event & Weaknes reporting	evidence needs to be added by IT	IM 3.1 Advanced
			evidence needs to be added by IT	IM 3.2 Advanced
			evidence needs to be added by IT	IM 3.3 Advanced
	Information System Continuty Policy	SC 1 Information System Continuty Policy	evidence needs to be added by IT	SC 1.1 Policy
		SC 2 Information system continuty planning	evidence needs to be added by IT	SC 2.1 Advanced
			evidence needs to be added by IT	SC 2.2 Advanced
			evidence needs to be added by IT	SC 2.3 Advanced
	Data Privacy & Protection	Data Privaly new policy need to be created and respective evidence must be provided	evidence needs to be added by IT	Policy creation
	Cloud Security	Cloud Security Policy Need to be created & respective evidence must be provided	evidence needs to be added by IT	Email & Hosting Location screenshot & Digital Marketing video cloud location screenshot
	Supply Chain Management	Supply Chain Management Policy	evidence needs to be added by IT	Write to audit & Non disclosure agreement & Federal & Local government requirements & Information security Policy requirements & Change of Scope
	Mobile & Portable Device security Policy	Mobile & Portable Device security Policy	evidence needs to be added by IT	Policy Practical evidence by installing software in mobile devices,tablets etc for mobile security

			•	
Section B	Log Management Policy	Log Management Policy	evidence needs to be added by IT	NTP evidence of firewall Log sheets and checklists maintained Log Management policy
	Log Management Policy	Policy Need to be created	evidence needs to be added by IT	CCTV aacess Log, Server Access Log, Bio Medical or Any third party vender visit log, CCTV or any third party vendor or police visit log, Fire Drill evacuation log report, Insta User Session Log, Publicholdays or Off Days working log Temprature logs for the bio medical room and Server room, Visitor Logs, Visitor Pass
Prepared by:	**Nisha Viswanathan**	**Review by:**		
Date:	**11-08-2024**	**Date:**		