INFORMATION CLASSIFICATION TABLE

Class	***Harm***	***Information Type***	***Security Zones****	***Copying***	***Destruction***
Restricted **R**	• Harm to operations of facilities or security systems • Immediate harm to health and safety of patients, clients, or staff • Loss of source record and accountability	• Information describing security systems, access codes, etc. • Personal information that would likely cause or allow a person to harm themselves or specific staff, or clients • Back-up of essential records	*Network:* Restricted *Physical:* Restricted	No copying	Supervised on-site shredding or data wiping and destruction logged
Confidential **C**	• Harm to privacy of patients, clients, staff • Economic loss for public body or third parties • Damage to credibility or service integrity of public body • Legislative sanctions • Loss of source record and accountability	• All personal information • Employee information • Information given in confidence or under privilege • Third party business information • Deliberations, investigations, advice, decisions • Security audit tools	*Network:* Internal preferred; External by approval *Physical:* Internal preferred; External by approval; Restricted for archival	Only for backup or when access to original impractical; destroy immediately after use	Confidential shredding or data wiping and destruction logged
Internal Use **I**	Loss of source record and accountability	• Staff circulars • Administrative records available to public upon request, e.g., completed decisions, policies, reports • Source records of public information	*Network*: Internal or External *Physical*: Internal or External; Restricted for archival	No restrictions	Destruction logged
Public **P**	No identified harms	• Published materials such as pamphlets, newsletter, annual reports • Public information such as directories or web sites	No restrictions	No restrictions	No restrictions

PHYSICAL ZONES REQUIREMENTS TABLE

Security Zone	Requirements			
	Authorization	***Barriers to Zone***	***Environment***	***Monitoring***
RESTRICTED *Server rooms* *HR records areas*	• Trusted user function-based by Managing Director • Unauthorized trusted user case-based by authorized person • No public access	• Area only accessed only from Internal zone • Locked and accessible to authorized persons only with ID • Unauthorized visitors accompanied by authorized persons	Archives standard	• Staff or CCTV surveillance • All access logged
INTERNAL *Admin/technical areas* *Unit desks/reception areas* *Individual examination areas*	• Trusted user function-based • Unauthorized trusted user by context • Public access case-based by authorized person	• Areas access from External or Public Zones • Locked and restricted to authorized persons with ID • Public visitors accompanied by authorized persons • Sound barriers	Normal standard	• Staff surveillance • Non-authorized access logged
EXTERNAL *Examination rooms* *Off-sites workplaces: (staff cars/ homes)*	Trusted and Public user by context	• Areas accessed from Public or Internal Zones • Locked areas or containers; marked boundaries • Public visitors unaccompanied but without access to information • Low verbal communication	Normal standard	Unlocked areas under staff surveillance
PUBLIC *Waiting areas*	None	Open but locked off-hours	May be uncontrolled	Staff or CCTV surveillance

- *Trusted User*: a staff member or third party accessing an Public Body network, resource, or building in compliance with Public Body security policy and under agreement
- *Public User*: a user not under Public Body policy or agreement

NETWORK ZONES REQUIREMENTS TABLE

Security Zone	**Requirements**					
	User	***Connection***	***Firewall Barriers***	***Zone Authentication***	***Encryption***	***Equipment***
RESTRICTED	Restricted	Internal to LAN/dedicated line		1 factor		
INTERNAL						
Status 1	Trusted	Internal to LAN/dedicated line	Internal DMZ	1 factor	None	Public Body
Status 2	Trusted	Ext. via internet	External, Internal DMZ	1 factor	Strong	Public Body / External
	Public		No Access			
EXTERNAL	Trusted	Ext. internet to Extranet	External DMZ	2 factor	Strong	Public Body / External
	Public		No Access			
PUBLIC	Public		Full Access			

- *Trusted User*: a staff member or third party accessing an Public Body network, resource, or building in compliance with Public Body security policy and under agreement
- *Public User*: a user not under Public Body policy or agreement