

- This form is to allow external party/ vendor access to specific WH IT Systems and should be completed & signed by the Western Health Authorising Manager. Details of all servers to be accessed must accompany this request.
- Scan and email the completed form to WH Service Desk (servicedesk@wh.org.au).
- Western Health Service Desk will notify the account details via e-mail either to the requestor or the Authorising Manager
- Access will be granted *within 5 business days* of the Service Desk receiving the correctly completed form.

External Party/ Vendor Account Details to complete (PLEASE PRINT CLEARLY IN BLOCK LETTERS)

Company Name:			
Full Name:			
Given Names		Last Name/ Surname	
Email Address:(<i>Contac</i>	t email address – must be	e organisation em	ail)
Business Tel:	Mobile:		(required for account verification)
Business Address:			
Country:			
Start Da	te: / /	Ι	End date: / / (if applicable)
External Party's Signatu	re:		Date: / /
Note: With your signature,	you have read, understood ar	nd agreed with the "C	Conditions of Use of Western Health DTS" below.
Western Health Auth	norising Manager to c	<u>omplete (</u> PLEASE	PRINT CLEARLY IN BLOCK LETTERS)
Manager:			
Given Names		Last Name/ Surname	
Position:		Department:	
Business Tel:	Mobile:	Emai	Address:
Manager's Signature:			Date: / / Fax:

Scan and email the completed form to Western Health ServiceDesk (servicedesk@wh.org.au)



Secure Remote Access for External Party/ Vendor *** Conditions of Use of Western Health DTS***

Declaration for requesting Secure Remote Access

Please ensure you read and understand the following conditions prior to signing.

Confidentiality of Information

You shall be responsible as an external party/ vendor or healthcare professional to abide with the **ethical** and **contractual** requirements, for maintaining the confidentiality of **ALL** data accessed on Western Health systems. *Note: Downloading or printing of information to remote locations (e.g., home PCs/ printers) is prohibited.*

Confidentiality of Passwords

Your personal password must be regarded as confidential and absolutely protected. Your password is a 'stamp' that identifies your access, actions and activities in the network and computer system(s). It must not be divulged to others because the responsibility for actions performed under your login and password shall remain yours.

Password Security

No account holder is to attempt to bypass or defeat the security systems or attempt to obtain the use of passwords or privileges issued to other account holders. Should such attempts be uncovered, disciplinary action(s) will follow, including reporting the matter to the police.

Software Security

You shall not contribute to any risk or exposure of the systems to copyright breach. This applies to both applications developed by the hospital or commercially purchased.

Hardware Security

You shall not contribute to any risk or exposure of the systems to hardware security. You shall ensure, as far as possible within your role in the hospital that the computer equipment is protected from theft, damage and unauthorised access.

Reporting Lapses of Security

You shall report to the Western Health Authorising Manager any known or observed attempts to break security, data breach/ theft or to gain unauthorised computer access.

Change Management

You shall abide by Western Health's Change Management policy to lodge a Request for Change for any change to be carried out on the system under your control.

Termination of Access

You shall be responsible to inform us to terminate the access account (s) when they are no longer required. This is to ensure that the account(s) are not abused by some other party whilst you are still responsible for the remote access by your organisation.

