

Remote Access Form (Non-Employees Only)

INSTRUCTIONS

SPONSOR – HDS MANAGER WHO IS REQUESTING AND AUTHORIZING ACCESS FOR THE RECIPIENT

- Facilitate completion of this form and ensure that a System Access Form has been completed.

RECIPIENT – HDS NON-EMPLOYEE WHO IS RECEIVES ACCESS TO HDS SYSTEMS

- Work with sponsor to gain access to, read, and fully understand any relevant policies, guidelines, and terms being acknowledged.
- Fill and submit this form to SPONSOR prior to using remote access services.

HELPDESK – HDS CONTACT FOR ANY QUESTIONS REGARDING THIS FORM

- Confirm attachment of completed RAF form to tickets which request access for HDS non-employees
- Verify that remote access usage requirements specified in the RAF match the requirements stated in the Sponsor Access Form (SAF).
- Facilitate completion or corrections of any required fields

REMOTE ACCESS USAGE

- ☐ Virtual Desktop (Citrix Xen)
- ☒ Virtual Private Network (VPN)
- ☐ Mobile VPN

RECIPIENT ACKNOWLEDGEMENT

I acknowledge that I have read and understand Appendix A - Terms and Conditions ☒

I acknowledge that I have read and understand Appendix B ☒

HDS Manager Name HDS Manager Title

Recipient Name Date

APPENDIX A - TERMS AND CONDITIONS

As an Hitachi Data Systems (HDS) mobile user, I acknowledge and agree:

- That I will be using my personal mobile device or accessing remotely HDS network for conducting HDS' business.
- To obey federal, state, and local laws and ordinances when using my mobile device, including all such laws and regulations pertaining to the use of cell phones while driving. I further understand that, if I am charged with traffic violations resulting from the use of my mobile device while driving, I will be solely responsible for all liabilities that result from such action.
- To use my mobile device in a safe and responsible manner while conducting HDS business.
- That I am responsible for providing and maintaining my mobile device, cellular service plan for my device, any necessary equipment and accessories for my device.
- That I am solely responsible for any and all expenses incurred from the use or loss of my mobile device and that HDS has no financial liability for my mobile device, service plan, and any necessary equipment and accessories.
- That IT will install an agent on my mobile device to provide security and remote management to protect my business/ personal data by erasing HDS specific contents from my device in the event of a security breach or notification from the end-user that the device has been lost/stolen/misplaced.
- A password and auto lock feature will be maintained on the mobile device.
- That I will keep the operating system of my device current and will install all available updates.
- HDS reserves the right to wipe out the device in case of security violation or tampering.
- HDS has the right to suspend e-mail transmission to a mobile device that does not meet the minimum password standards or if the OS has been compromised (i.e. jail broken, rooted, infected with a virus, etc.).
- I have read and understand Appendix B - HDS Access Authorization & Agreement to HDS Network.

Appendix B - Access Authorization and Agreement

- Mobile access is granted for the purpose of performing HDS business. Sharing this access is prohibited. Any HDS related information, which you have created or you have been granted access, is your responsibility to protect.
- All remote access software, settings or configuration is considered to be confidential. Remote users shall not share, copy or modify, remote access software. The configuration file supplied by the Helpdesk either with the client or separately contains encrypted authentication information for accessing HDS. At no time is the remote access recipient authorized by HDS to share this information with any other individual or companies.
- While a remote connection is established to the HDS' network, your computer will become an extension to the HDS' network. Even when not connected to the HDS' network, your computer may contain proprietary HDS' information that you are responsible to protect.
- All data files, devices and other physical matter which relate to the business of HDS and its subsidiaries or affiliates, and which you may originate, author, or which may come into your possession, during the course of your business with HDS are the property of HDS.

Logical and Physical Protection

- In order to prevent unauthorized access, damage and interference to IT services, all mobile devices and related equipment must be secured. Computer systems must not be left logged in and unattended. Screen-savers should be set according to HDS Security standards. All mobile devices must be secured by a password. The auto lock feature must be enabled to ensure a password will be required for each use.
- Report immediately any loss or theft of HDS proprietary information. This is done by filing an incident report form. Computer malware pose a threat to HDS systems. It is important that all computer users adhere closely to the following anti-malware procedures and measures:
 - A virus scanner / malware protection must be installed on all computing devices that connect to HDS' network.
 - Those users without a virus scanner / malware protection installed may be denied access to the network or VPN without notice.
 - If malware activity is detected originating from a remote device, access to the network for that device will be immediately terminated without notice.
 - Virus scanning occurs on all production servers on a continuous basis.
 - Any files or programs found to contain a virus may be cleared of the virus or deleted from the system without notice.

Access and Application Use – E-mail

- HDS e-mail system must be used in a manner consistent with HDS standards of business conduct. Misuse of the e-mail system or any breach of Hitachi Data Systems use policies may put both HDS and you at risk for legal action and/or prosecution.
- If you observe any misuse of the e-mail system please immediately notify your HDS sponsor or the HDS Help Desk as soon as possible.
- All messages composed, sent or received on the system are also the property of HDS and may be reviewed for content. HDS assumes no responsibility for any legal damages resulting from your use and/or misuse of the e-mail system.

Access Termination

- For any non-HDS employee, access is limited, the duration is set by the Sponsor Access Form (SAF).
- Laws and Regulations
- Users must follow all laws and regulations of the country /state where they are physically located when they use their mobile device.

Appendix B - Access Authorization and Agreement (Cont'd.)

Security Breaches

➤ Specific breaches of confidentiality, whether inside or outside HDS will be regarded as serious misconduct, which will result in remote access privileges to be terminated immediately and written notification sent to the manager or HDS sponsor. Users who have access to HDS proprietary information must report promptly any actual or suspected incidents to their HDS Sponsor and/or ITSecurity@hds.com.

Monitoring / Unauthorized Activities

➤ HDS IT Network Group monitors all accounts for unauthorized activity. Unauthorized activity will cause privileges to be terminated immediately. Any damages resulting from unauthorized activity will be grounds for legal action. HDS reserves the right to terminate access without notice.