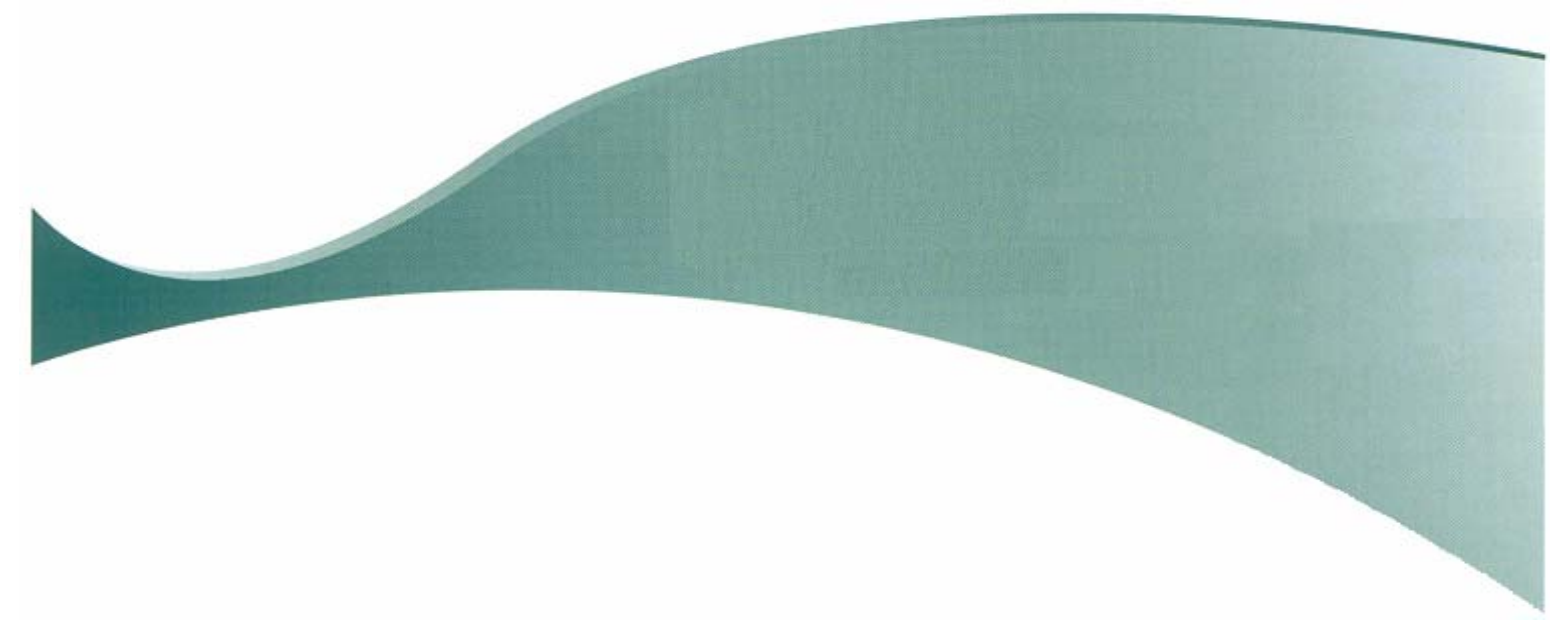
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Third Party
Network Access Agreement



Version 2.0

Please ensure you check the HSE intranet for the most up to date version of this document.
http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/

1.0 Purpose

The purpose of this agreement is to outline the specific terms and conditions governing the access and use of the Health Service Executive (HSE) network and information technology resources by the third party.

The Third Party Network Access Agreement is an addendum to the HSE Standard Terms for Services & Supplies (or title of bespoke contract) which governs this agreement.

This agreement is dated _____ and made between the Health Service Executive and the following Third Party:

Company name: _____

Address: _____

_____

_____

Phone number: _____

Fax: number: _____

2.0 Definitions

- Third parties are defined as any individual, consultant, contractor, vendor or agent not registered as a HSE employee.
- Third party access is defined as all local or remote access to the HSE network for any purpose.
- HSE network includes all data, applications, systems, services, infrastructure and computer devices which are owned or leased by the HSE.
- Mobile computer devices are defined as any handheld computer device, including but not limited to laptops, notebooks, tablet computers, smartphone devices (e.g. PDA, iPhone and Blackberry enabled devices, etc).
- Removable Storage devices are defined as any optical or magnetic storage device or media, including but not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick/pen/keys), external/portable hard drives.

3.0 Terms & Conditions

1. The third party may only use the network connection for approved business purposes as outlined in their ***Third Party Access Request Form***. The use of the network connection for unapproved purposes, including but not limited to personal use or gain is strictly prohibited.

2. The third party may only use access methods which have been defined by the HSE ICT Directorate.

3. The third party must ensure that only their employees that have been nominated by the third party and approved by the HSE in advance, have access to the network connection or any HSE owned equipment

4. The third party shall be solely responsible for ensuring its nominated employees are not security risks, and upon request from the HSE, the third party will provide the HSE with any information reasonably necessary for the HSE to evaluate security issues.

5. The third party will promptly inform the HSE in writing of any relevant employee changes. This includes the rotation and resignation of employees so that HSE can disable their usernames and remove / change passwords in order to secure its resources.

6. As part of the annual service agreement review the third party will provide the HSE with an up to date list of their employees who have access to the network connection or any HSE owned equipment.

7. The third party is solely responsible for ensuring that all usernames and passwords issued to them by the HSE remain confidential and are not used by unauthorised individuals. The third party must immediately contact the HSE if they suspect these details have been compromised.

8. The third party will be held responsible for all activities performed on the HSE network while logged in under their usernames and passwords.

9. The third party must ensure at all times that all computer devices used by them to connect to the HSE network have reputable up to date anti-virus software and the appropriate security patches installed.

10. Only in exceptional circumstances and with the prior written approval of the HSE should the third party hold HSE information on mobile computer devices or removable storage devices. Should the business requirements necessitate the third party to store HSE information on mobile computer devices or removable storage devices, the third party must ensure that only the absolute minimum amount of information as is absolutely necessary is stored on the mobile computer device or

removable storage device and the information is securely deleted when it is no longer required. The third party must ensure that all HSE information stored on mobile computer devices and removable storage devices belonging to the third party is encrypted in accordance with the *HSE Encryption Policy*. Under no circumstance encrypted or otherwise should HSE information be stored by the third party on USB memory keys/sticks.

11. The third party must ensure that all mobile computer devices used by them to connect to the HSE network, are used in such a way that information belonging to the HSE is not displayed to unauthorised individuals or the general public.

12. The third party must ensure that all their computer devices connected to the HSE network are not connected to any other network at the same time, with the exception of networks that are under the complete control of the third party.

13. When the third party is connected to the HSE network they should not leave their computer devices unattended.

14. The third party must ensure that when they are connected to HSE network their activity does not disrupt or interfere with other non-related network activity.

15. All third party computer devices used to connect to the HSE network must, upon request by HSE be made available for inspection.

16. The third party network connection will by default be granted read / execute privileges only. All requests for increased privileges must be submitted in writing to the HSE where they will be considered on a case by case basis.

17. For security reasons all third party remote access accounts except those providing 24*7 support will be switched off (de-activated) by default. The third party will be required to email (can be followed by phone) the HSE ICT Directorate requesting that their account be switched-on (activated) for a stipulated period.

18. Third party remote access accounts providing 24*7 support will remain open at all times for diagnostic purposes. However the third party will be required to email the HSE ICT Directorate each time the account is used.

19. The third party must obtain the written consent of the HSE before implementing any updates or amendments to the HSE network, information systems, applications or equipment. All approved updates and amendments implemented by the third party must be made inline with the HSE Change Management policies and procedures.

20. The third party must ensure all software is scanned and cleared of all viruses and other forms of malicious software before it is installed on any HSE information systems, applications or equipment. The third party will be held responsible for all

disruptions and damage caused to the HSE network, information systems, applications or equipment which is traced back to infected software installed by the third party.

21. The third party and their employees must comply with all Irish, European and HSE rules and regulations concerning safety, environmental and security operations while on-site at a HSE facility. All third party personnel must carry photographic identification with them when they are on-site at a HSE facility.

22. Where the third party has direct or indirect access to HSE information, this information must not be copied, divulged or distributed to any other party without the prior written approval of the HSE

23. The third party must report all actual and suspected security incidents to the HSE immediately.

24. The third party must manage and process all HSE information which they acquire from the HSE in accordance the *Data Protection Act 1988*, the *Data Protection (Amendment) Act 2003* and EU Directive 2002/58/EU.

25. The HSE reserves the right to:

- Monitor all third party activity while connected (local and remote) to the HSE network.
- Audit contractual responsibilities or have those audits carried out by a HSE approved third party
- Revoke the third parties access privileges at any time.

26. On completion of this contract the third party must return all equipment, software, documentation and information belonging to the HSE.

27. Any violations of this agreement by the third party, may lead to the withdrawal of HSE network and information technology resources to that third party and/or the cancellation of any contract(s) between the HSE and the third party.

I agree to abide by the terms and conditions of this agreement at all times

Signed (On behalf of the Third Party):

Company Name: _____

Authorised Signature: _____

Name (Printed): _____

Title or Position: _____

Date: _____