TGMC
Terrebonne General Medical Center

Terrebonne General Medical Center Policy and Procedure

Title: Remote Access User Policy	**Control No.: 8230-Technical**	**Version: 1**
Replaces: Not Set		
Policy Owner: Tyler Dupre (Security Administrator),Information Technology		
Reviewers: Jeff Sardella (Director), Steven Domangue (Technical Operations Manager) Information Technology		
Approvers: Diane Yeates (Chief Operating Officer) Administration	**Date Approved: 10/25/2016**	**Date Last Reviewed: 10/25/2016**

Purpose:

The purpose of this policy is to establish uniform security requirements for all authorized users who require remote electronic access to Terrebonne General Medical Center's network and information assets from any host. The guidelines set forth in this policy are designed to minimize exposure to damages that may result from unauthorized use of Terrebonne General Medical Center's resources and confidential information. These legally mandated controls are in place to preserve, the integrity, availability and privacy of data.

This policy applies to all Terrebonne General Medical Center employees, contractors, vendors and agents with a TGMC-owned, personally-owned, or company owned computer or workstation used to remotely connect to the Terrebonne General Medical Center network for the purpose of conducting its operations, treatments and payments.

Policy:

By using remote access with personal equipment, users must understand that their machines are a de facto extension of TGMC network, and as such are subject to the same rules and regulations that apply to TGMC owned equipment.

Policy Statements

1. It is the responsibility of Terrebonne General Medical Center employees, contractors, vendors and agents with remote access privileges to Terrebonne General Medical Center's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Terrebonne General Medical Center.
2. The Terrebonne General Medical Center user is responsible to ensure any of their family members do not access any Terrebonne General Medical Center data, do not perform illegal activities, and do not use the Terrebonne General Medical Center access for

outside business interests. The user bears responsibility for the consequences should the access be misused.

3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Terrebonne General Medical Center's network:
    1. *Computer Acceptable Use Policy*
    2. *Password and Access Policy*
    3. *Internet Cyber Conduct Policy, if applicable*
    4. *Email Policy, if applicable*
    5. *Wireless Device Email Policy, if applicable*
4. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. At no time should any Terrebonne General Medical Center user provide their login or email password to anyone, not even family members.
5. Terrebonne General Medical Center users and contractors with remote access privileges must ensure that their Terrebonne General Medical Center-owned or personal computer or workstation, which is remotely connected to Terrebonne General Medical Center's corporate network, is not connected to any other network at the same time, with the exception of business or personal networks that are under the complete control of the user.
6. Terrebonne General Medical Center employees and contractors with remote access privileges to Terrebonne General Medical Center's corporate network must not use non-Terrebonne General Medical Center email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Terrebonne General Medical Center business, thereby ensuring that official business is never confused with personal business.
7. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
8. All hosts that are connected to Terrebonne General Medical Center internal networks via remote access technologies must use the most up-to-date anti-virus software this includes personal computers.
9. Personal equipment that is used to connect to Terrebonne General Medical Center's networks must meet the requirements of Terrebonne General Medical Center-owned equipment for remote access.
10. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Terrebonne General Medical Center production network must obtain prior approval from the Information Technology Department.
11. Do not save PHI (Personal Health Information) to desktop, hard drive, or other storage on personal devices. These are not protected by TGMC security policies.
12. Remote users will be automatically disconnected from TGMC network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
13. The remote user is limited to an absolute connection time of 24 hours unless related to continued operations or treatment and approved by the Security Officer in advance.

Procedure:

Adding New Remote Access

1. Refer to *TGMC Authorization and Access Policy* for roles preapproved for remote access via TGMC owned equipment or personal/company owned equipment.

2. Providers must complete the Request for Information System Access, sign the confidentiality agreements and review applicable policies prior to obtaining approval from Department Director or Medical Staff Coordinator to obtain remote access connection.
3. Any contractor, vendor or associate that is granted access must complete the Request for Information System Access form, complete a Business Associates Agreement as part of their contracting process and sign a confidentiality agreement which includes review of applicable TGMC policies prior to being granted access. A termination date is assigned based upon contract terms that curtails access. This termination date can be reviewed and revised as circumstances change but must be completed prior to being granted access.

Terminating Access of Users

1. Refer to *TGMC Authorization and Access Policy* for termination procedures for employee access.
2. Medical providers and staff office remote access will be terminated for all accounts that have not had activity for more than 6 months and will be included for automatic termination.
3. All contractors, vendors and other partners that perform treatment or operations for TGMC will have an expiration date that corresponds to their contract. Any extensions or contract renewals will require another Information Services Request form with a new expiration period to be approved.

Definitions:

Dual Homing Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the corporate network via a local Ethernet connection, and connecting to Gmail or other Internet service provider (ISP). Being on a Terrebonne General Medical Center-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to connect to Terrebonne General Medical Center and an ISP, depending on packet destination.

Remote Access Any access to Terrebonne General Medical Center's corporate network through a non-Terrebonne General Medical Center controlled network, device, or medium.

Split-tunneling Simultaneous direct access to a non-Terrebonne General Medical Center network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Terrebonne General Medical Center's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

References:

TGMC Acceptable Use Policy
TGMC Internet Cyber Conduct Policy
TGMC Email Policy
TGMC Wireless Device Email Policy
TGMC Password and Access Policy
TGMC Business Associates Agreement Policy