



## Security Policies for TwinNET

SOP Title: Security Policies for TwinNET	SOP No. 1.	Version No. Draft 4.	Valid from (date): 2005-09-01
Compiled by	2005-06-16	Jon Roy Johansen	
Approved by (date and name):	2005-08-24	Jon Roy Johansen	
Approved by (date and name):	2005-08-30	Jan-Eric Litton	



# Index

<b>SECURITY POLICIES FOR TWINNET .....</b>	<b>1</b>
<b>INDEX.....</b>	<b>3</b>
<b>1. GENERAL .....</b>	<b>6</b>
1.1. Purpose.....	6
1.1.1. Related documents:.....	6
1.2. Updating this document.....	7
1.3. Definitions .....	7
1.4. Scope .....	8
1.5. Policy.....	8
1.5.1. General network topology.....	8
1.6. Enforcement .....	9
<b>2. DATA ACCESS AND STORAGE .....</b>	<b>10</b>
2.1. Purpose.....	10
2.2. Scope .....	10
2.3. Policy.....	10
2.3.1. Gaining access .....	10
2.3.2. After the research has ended .....	10
2.4. Enforcement .....	10
<b>3. SECURE COMMUNICATION.....</b>	<b>11</b>
3.1. Purpose.....	11
3.2. Scope .....	11
3.3. Policy.....	11
3.4. Enforcement .....	11
<b>4. AUDITING .....</b>	<b>12</b>
4.1. Purpose.....	12
4.2. Scope .....	12

- 4.3. Policy..... 12
  - 4.3.1. Onsite Point of Contact ..... 12
  
- 5. EMAIL..... 13**
- 5.1. Purpose ..... 13
- 5.2. Scope ..... 13
- 5.3. Policy..... 13
  
- 6. DMZ..... 13**
- 6.1. Definitions ..... 13
- 6.2. Purpose ..... 13
- 6.3. Scope ..... 14
- 6.4. Policy..... 14
  - 6.4.1. General Network Design ..... 14
- 6.5. Ownership and Responsibilities ..... 14
  - 6.5.1. General Configuration Requirements..... 15
  
- 7. PASSWORD POLICY ..... 17**
- 7.1. Overview ..... 17
- 7.2. Purpose ..... 17
- 7.3. Scope ..... 17
- 7.4. Policy..... 17
  - 7.4.2. Guidelines..... 18
- 7.5. Password Protection Standards..... 19
- 7.6. Enforcement ..... 20
  
- 8. REMOTE ACCESS POLICY ..... 21**
- 8.1. Purpose ..... 21
- 8.2. Scope ..... 21
- 8.3. Policy..... 21
  - 8.3.1. General ..... 21
  - 8.3.2. Requirements ..... 21
  
- 9. ROUTER SECURITY POLICY ..... 23**

- 9.1. Purpose ..... 23
- 9.2. Scope ..... 23
- 9.3. Policy ..... 23
- 10. SERVER SECURITY POLICY ..... 24**
- 10.1. Purpose ..... 24
- 10.2. Scope ..... 24
- 10.3. Policy ..... 24
  - 10.3.1. Ownership and Responsibilities ..... 24
  - 10.3.2. General Configuration Guidelines ..... 24
- 10.4. Monitoring ..... 25
- 10.5. Compliance ..... 25
- 10.6. Enforcement ..... 25
- 11. VIRTUAL PRIVATE NETWORK (VPN) POLICY ..... 26**
- 11.1. Purpose ..... 26
- 11.2. Scope ..... 26
- 11.3. Policy ..... 26
- 11.4. Enforcement ..... 26
- 12. WIRELESS COMMUNICATION POLICY ..... 27**
- 12.1. Purpose ..... 27
- 12.2. Scope ..... 27
- 12.3. Policy ..... 27
- 12.4. Enforcement ..... 27
- 13. BREACH OF SECURITY POLICY ..... 28**
- 13.1. Purpose ..... 28
- 13.2. Scope ..... 28
- 13.3. Policy ..... 28
- 13.4. Enforcement ..... 29

# 1. General

## 1.1. Purpose

The purpose of this document is to provide general guidelines for secure communication through the Internet under the conditions and rules supplied by the Ethical Core of the GenomEUtwin.

GenomEUtwin is a European Commission funded collaboration between Twin Registries from the Netherlands, Denmark, Norway, Sweden, Finland, Italy, UK and Australia with the aim to identify genetic variants associated with common diseases by pooling potentially over 600 000 twin pairs.

The TwinNET (GenomEUtwin collaboration network, see also 6.1) Security Group will enforce the rules. E-mail to the Security Group is; [twinnet@genomeutwin.org](mailto:twinnet@genomeutwin.org). The TwinNET Security group is a working group under the database core in GenomEUtwin.

The member of the TwinNET Security Group are;

Role	Name	E-mail	Country
Head of group	Jon Roy Johansen	<a href="mailto:jon@fhi.no">jon@fhi.no</a>	Norway
Member	Harry Beeby	<a href="mailto:harryB@qimr.edu.au">harryB@qimr.edu.au</a>	Australia
Member	Lars Hvidberg	<a href="mailto:lhvidberg@health.sdu.dk">lhvidberg@health.sdu.dk</a>	Denmark
Member	Ahokas Juri	<a href="mailto:juri.ahokas@ktl.fi">juri.ahokas@ktl.fi</a>	Finland
Member	Juha Muilu	<a href="mailto:juha.muilu@helsinki.fi">juha.muilu@helsinki.fi</a>	Finland
Member	Saharinen Juha	<a href="mailto:juha.saharinen@ktl.fi">juha.saharinen@ktl.fi</a>	Finland
Member	Timo Miettinen	<a href="mailto:timo.a.miettinen@helsinki.fi">timo.a.miettinen@helsinki.fi</a>	Finland
Member	Nieuwboer RT	<a href="mailto:RT.Nieuwboer@psy.vu.nl">RT.Nieuwboer@psy.vu.nl</a>	Holland
Member	Wijk, H.J. van der	<a href="mailto:H.J.van_der_Wijk@lumc.nl">H.J.van_der_Wijk@lumc.nl</a>	Holland
Member	Eugenio Carrani	<a href="mailto:carrani@iss.it">carrani@iss.it</a>	Italy
Member	Tatjana Dukic	<a href="mailto:t.dukic@jumpy.it">t.dukic@jumpy.it</a>	Italy
Member	Martinsen, Tommy	<a href="mailto:Tommy.Martinsen@fhi.no">Tommy.Martinsen@fhi.no</a>	Norway
Member	Johan Söderberg	<a href="mailto:johan.soderberg@meb.ki.se">johan.soderberg@meb.ki.se</a>	Sweden
Member	Mats Johansson	<a href="mailto:mats.jonsson@medsci.uu.se">mats.jonsson@medsci.uu.se</a>	Sweden
Member	Gunnar Petersson	<a href="mailto:gunnar.petersson@meb.ki.se">gunnar.petersson@meb.ki.se</a>	Sweden

### 1.1.1. Related documents:

1. GenomEUtwin: Agreement for sharing and access to biological sample and GenomEUtwin data – Terms and Conditions.

2. Proposal from the GenomEUtwin Data Access and Security (DAS) working group regarding routines and policies for data access, ownership, use and security in GenomEUtwin.

3. EU IPR helpdesk comments June 2005; GenomEUtwin Data Access and Security.

[http://www.genomeutwin.org/member/cores/docs/eu\\_ipr\\_helpdesk\\_comments\\_june\\_2005.pdf](http://www.genomeutwin.org/member/cores/docs/eu_ipr_helpdesk_comments_june_2005.pdf)

4. A Björklund and J-E. Litton. Data Format and Variable Standard for GenomEUtwin's Phenotype Database Prototype, Version: 4.0 (2004)

[http://www.genomeutwin.org/member/cores/db/docs/GenomEUtwin\\_Data\\_Format4\\_0.pdf](http://www.genomeutwin.org/member/cores/db/docs/GenomEUtwin_Data_Format4_0.pdf)

## 1.2. Updating this document

It is the responsibility of the head of the security group to ensure that the participating always has access to the latest version of this document. This will be done by sending all updates to the [twinnet@genomeutwin.org](mailto:twinnet@genomeutwin.org) e-mail group which contains at least one member from each participating site responsible for the site's TwinNET security

The head of the security group, or a person delegated this responsibility, will be responsible for updating this document as necessary.

Any comments regarding changes to, or interpretations of, the contents should be sent to the head of the security group.

## 1.3. Definitions

TwinNET = GenomEUtwin collaboration network. With the following partners:

- The Netherlands Twin Registry, Dept of Biological Psychology, Vrije University, Amsterdam
- Department of Molecular Medicine, National Public Health Institute, Helsinki, Finland
- Finnish Twin Cohort Study, University of Helsinki, Finland
- Finnish Genome Center, University of Helsinki, Finland
- Department of Medical Sciences, Uppsala University, Sweden
- Swedish Twin Registry, Karolinska Institutet, Stockholm, Sweden
- Danish Twin Registry, University of Southern Denmark, Odense, Denmark
- Italian Twin Registry, Istituto Superiore di Sanità, Rome, Italy
- Norwegian Twin Registry, The Norwegian Institute of Public Health, Oslo, Norway
- Department of Epidemiology and Public Health, University of Belfast, UK
- Leiden University Medical Centre, Leiden, the Netherlands
- Twin Research and Genetic Epidemiology Unit, St. Thomas' Hospital, London, UK
- Australian Twin Registry, Queensland Institute of Medical Research, Brisbane, Australia

New partners may/will be added at any time.

Site = One of the TwinNET partners

Steering Group = GenomEUtwin Steering Group (GSG)

Security Group = The TwinNET Security Group is a sub-group of the Database Core, appointed by the GenomEUtwin Steering Group

## **1.4. Scope**

This policy applies to all TwinNET sites.

## **1.5. Policy**

Data must be stored so that unauthorized access is prohibited.

All databases and data sets maintained under the TwinNET are deidentified and do not contain any information that can be used to identify individuals participating in the studies. The only identifiers allowed which may be associated with subject or samples are randomized GenomEUtwin-identifiers (EUid, see also; A Björklund and J-E. Litton. Data Format and Variable Standard for GenomEUtwin's Phenotype Database Prototype, Version: 4.0 (2004) ). Geno- and phenotype data are stored in separate operational databases. The data may be combined for the sole purpose of analysis as described in an accepted manuscript proposal and then stored according to specified rules (See data access and security, J. Harris et al. and related documents).

Geno- and phenotype data can be accessed through a common federated data management system or through similar data integration software. Genotype and phenotype data are physically stored on different servers located at different sites. See also 1.3.1.

### **1.5.1. General network topology**

The data providers (twin centers) are connected to a HUB, which provides a single access point to the phenotype data which is located at different centers and to the genotype data (Figure 1). There are two HUBs. One in Helsinki and one in Stockholm. Genotype data can be stored on the server located in Helsinki HUB.

In the initial configuration connections and high-level connection protocols are limited to a minimum. The only allowed high level protocols between data providers (DPs) and HUB are database protocols such as ODBC, Net8 and DRDA. Connections must be made through encrypted VPN channels and terminated and firewalled according to rules described in following chapters. Connections can be opened only from the HUB side. Data providers are not allowed to open connections to each other or anywhere else, except into their local area networks as described in the VPN and firewall policy chapters. Access to HUB is blocked by firewalls and connections can be made only for administrative purposes using secure communication channels. Data are accessed through separate a web server or by login into a dedicated meta frame server, which are implemented according to security practices.

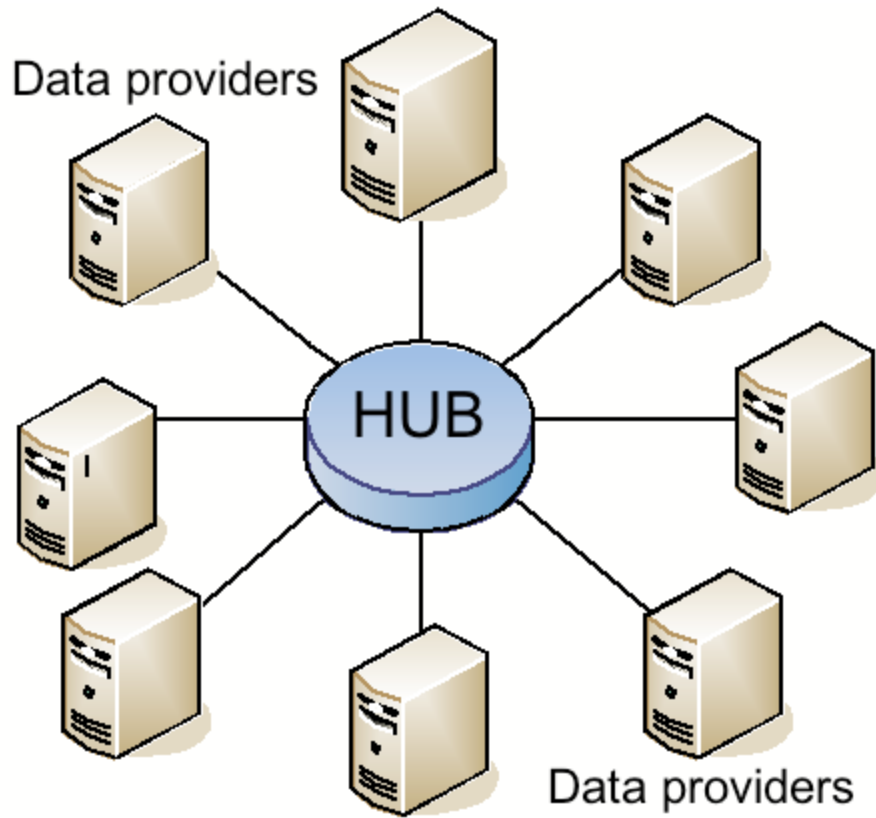


Figure 1

## 1.6. Enforcement

Any site found to be in violation to the policy described in 1.3 might be excluded from the TwinNET until the violation has ceased.

## **2. Data access and storage**

### **2.1. Purpose**

The purpose of this policy is to set guidelines for how data access is obtained and how data shall be treated after the research on the data has ended.

### **2.2. Scope**

This policy applies to all TwinNET sites.

### **2.3. Policy**

#### **2.3.1. *Gaining access***

Gaining access - as suggested by the EU helpdesk, all sites and GenomEUtwin, all personnel should sign a confidentiality agreement. After the Steering group has approved a manuscript (as a type of project) the group informs the administrator of one or both HUBs, depending on the need for information. The administrator(s) set up suitable permissions to the federated database and establishes a unique username and password for the project.

As a part of the application process the prime contact of the site requesting access will name one to three persons who will be responsible for retrieving data from the federated database to research projects on the site. One of these persons will be the prime contact to the HUB administrator.

Each project will have its own username and password. As the security group cannot be expected to know the participants of each project, the username/password will be given to one known and trusted contact at the site – the primary contact. The primary contact will then distribute the username/password to the project members which are allowed to access the federated database in a secure way.

The username and password will not be given to any other person.

#### **2.3.2. *After the research has ended***

When the research project has ended, usually after publication, a copy of all findings and data sets will be sent to the Helsinki databasegroup for safekeeping and storage. The databasegroup will ensure that the data are kept alive and readable. The data will be stored for a minimum of 15 years.

### **2.4. Enforcement**

Any site found to be in violation to this policy might be excluded from the TwinNET until the violation has ceased.

## **3. Secure communication**

### **3.1. Purpose**

The purpose of this chapter is to provide guidelines for secure communication through the Internet.

### **3.2. Scope**

This policy applies to all TwinNET sites.

### **3.3. Policy**

- AES 128 bit or stronger encryption will be used for SSL, IPsec and SSH tunnels.
- Preshared keys will be used for authentication.
- All IPsec communication shall be compatible with Cisco's versions of the protocols and all equipment used at the HUBs.

### **3.4. Enforcement**

Any site found to be in violation to this policy might be excluded from the TwinNET until the violation has ceased.

## **4. Auditing**

### **4.1. Purpose**

The purpose of this chapter is to set forth our agreement regarding network security scanning of TwinNET. The sites shall utilize hardware and/or software to perform electronic scans of networks, servers and firewalls.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents ensure conformance to TwinNET security policies
- Monitor user or system activity where appropriate.

### **4.2. Scope**

This policy covers all computer and communication devices used in connection to TwinNET. This policy also covers any computer and communications device that are present on the site's premises, but which may not be owned or operated by the site.

### **4.3. Policy**

Exhaustive logging shall be run continuously on all said equipment to monitor misuse, security breaches or failure to comply with the security policy. All logs shall be checked regularly.

When requested a report of all loggings shall be made available to the TwinNet Security Group.

#### **4.3.1. Onsite Point of Contact**

The site shall identify in writing a person, who is responsible for the auditing and available as an onsite resource if the TwinNet Security Group requires assistance.

## **5. Email**

### **5.1. Purpose**

The purpose of this section is to prevent the unauthorized or inadvertent disclosure of sensitive information.

### **5.2. Scope**

This policy covers automatic and manual email, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of TwinNET.

### **5.3. Policy**

Employees must exercise utmost caution if sending any data from the TwinNET servers to an outside network. Unless approved by the security group email will not be automatically forwarded to an external destination.

Exchange of encryption keys and similar types of information exchanges is not allowed using email.

## **6. DMZ**

### **6.1. Definitions**

TwinNET = GenomEUtwin collaboration network.

Satellite site = GenomEUtwin participating center that is connected to the GenomEUtwin network HUB.

HUB = Central connection point to which the GenomEUtwin participant connects. There are two HUBs within TwinNET, one to which all the phenotype satellite sites connect and one to which all the genotype satellite sites connect.

DMZ = De-Militarized zone.

TwinNET DMZ = Special purpose DMZ for the GenomEUtwin project.

VPN = Virtual Private Network.

### **6.2. Purpose**

This policy establishes information security requirements for all networks and equipment deployed in the different GenomEUtwin participants DMZs. Adherence to these requirements will minimize the potential risk to the GenomEUtwin of damage to public image caused by unauthorized use of the GenomEUtwin participant's resources, and the loss of confidential data and intellectual property.

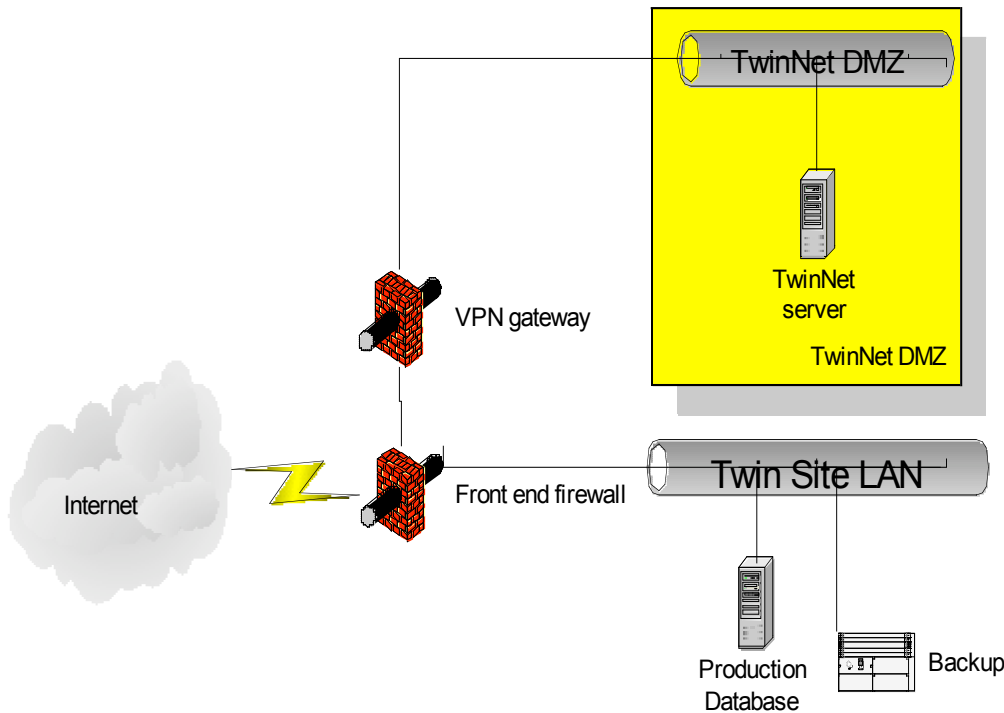
### 6.3. Scope

The GenomEUtwin participants networks and devices (including but not limited to routers, switches, hosts, etc) that are Internet facing and located outside the GenomEUtwin participants internet firewalls are considered part of the DMZs and are subject to this policy. This includes DMZs in primary Internet Service Provider (ISP) locations and remote locations. All existing and future equipment, which falls under the scope of this policy, must be configured according to the requirements and regulations outlined in this document. This policy does not apply to networks residing inside the GenomEUtwin participants Internet firewalls. Each GenomEUtwin participating site defines standards for these internal networks according to their specific needs.

### 6.4. Policy

#### 6.4.1. General Network Design

The minimum requirement in the network design should be to have the TwinNET DMZ in a separate zone and that zone must be protected by a firewall. The VPN gateway should be a separate dedicated device. The VPN encryption standard within TwinNET is IPSec (Cisco's implementation) and thus the VPN gateway must support it.



### 6.5. Ownership and Responsibilities

1. Each GenomEUtwin participants are responsible for assigning DMZ managers, point of contact and backup point of contact, and publish the point of contacts to the TwinNET Security Group.

2. Changes to the connectivity and/or purpose of existing DMZ and establishment of new DMZs must be requested to the GenomEUtwin Steering Group and approved by both the GenomEUtwin Steering Group and TwinNET Security Group.
3. Each GenomEUtwin participant must maintain a firewall device between his or her DMZ(s) and Internet.
4. The TwinNet Security Group reserves the right to terminate connections if a security concern exists.
5. Each GenomEUtwin participant will provide and maintain network devices deployed within their respective DMZ.
6. The TwinNET Security Group must record all GenomEUtwin address spaces and current contact information.
7. The GenomEUtwin participant's onsite point of contact is ultimately responsible for their DMZs complying with this policy.
8. Immediate access to equipment, system logs and system documentation must be granted to members of the TwinNET Security Group upon request, in accordance with the *Audit Policy*.
9. Each GenomEUtwin participant's onsite point of contact should provide necessary documentation upon request to the TwinNET Security Group.
10. The TwinNET security group will address non-compliance requests on a case-by-case basis.

### **6.5.1. General Configuration Requirements**

1. Each GenomEUtwin onsite point of contact is responsible for complying with the following related policies:
  - a. *GenomEUtwin Password Policy*
  - b. Each site should have an *Anti-Virus Policy* and implement it on its own DMZ
2. Deidentified data are replicated from the GenomEUtwin participant's master database on their Internal network to the database server in the TwinNET DMZ. These data are the only data exposed to the Internet.
3. All user accounts should be personal. No direct connection to anonymous or group accounts should be allowed.
4. All incoming and outgoing network communication to and from a TwinNET DMZs must always pass a firewall.
5. All incoming and outgoing network communication to and from a TwinNET DMZ must always be performed over a secure channel (e.g., SSH, SSL, IPSEC or equivalent).
6. The GenomEUtwin participants TwinNET DMZs must be physically secure and prevent unprivileged physical access.
7. The GenomEUtwin participant maintained firewall devices must be configured in accordance with least-access principles which means that as few people as possible should have access to the site's TwinNET systems.
8. No other data protocols than what is needed for database communication and TwinNET administration are allowed.
9. All TwinNET communication should be initiated from the HUBs.
10. Firewall configurations and any changes must be reviewed and approved by the TwinNet Security Group (including both general configurations and rule sets). The TwinNET Security Group may require additional security measures as needed.
11. All applicable security patches/hotfixes recommended by the vendor must be installed.

Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.

12. The GenomEUtwin participant's equipment should be tightened, i.e. services and applications not serving business requirements must be disabled.

## 7. Password Policy

### 7.1. Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may compromise the integrity of TwinNet's entire network. As such, employees at all participating sites (including contractors and vendors with access to TwinNet systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. It's the responsibility of the Database Manager to inform the End User of this password policy. A simplified version of this password policy should be handed out to all users.

### 7.2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

### 7.3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any TwinNet site, has access to the TwinNet network, or stores any non-public TwinNet information.

### 7.4. Policy

Unless specifically stated otherwise, the items in this section apply to both end users and system level accounts and passwords. Along with the requirements, section 7.4.1, all handling of user-level and system-level passwords should conform to the guidelines in section 7.4.2 as far as possible.

Requirements

#### 7.4.1.1. General standards

- Each end user must give written consent to follow the password policy and be properly approved by the Account administrator to receive a user account.
- Each user must have a unique username.
- No end user group accounts are allowed cf. guest accounts or shared accounts.
- Initial user and password information must be communicated in a safe way.
- Accounts should be locked after 5 consecutive unsuccessful login attempts.
- End user accounts should have a limited activation period.
- Unused accounts should be deactivated after 6 months.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All system-level passwords must be written down and stored in a locked safe to avoid system unavailability in case of emergencies.
- No passwords should ever be stored as clear text on any unprotected media.

#### **7.4.1.2. Password change standards**

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed at least every 3rd month.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 6th month.
- Passwords cannot be reused in 12 months.
- If a password is compromised or suspected to be compromised it should be changed as soon as possible.

#### **7.4.1.3. Password formulation standards**

- Password length must be 8 characters or more.
- Passwords must contain a mixture of at least alpha and numeric characters.
- Password constructions should follow the guidelines in section 7.4.2.1.

### **7.4.2. *Guidelines***

#### **7.4.2.1. General Password Construction Guidelines**

Passwords are used for various purposes at TwinNET. Some of the more common uses include: user level accounts, web accounts, screen saver protection, database accounts and local router/firewall logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or other)

The password is a common usage word such as:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "TwinNET", "sanjose", "sanfran" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#%\$%^&\*()\_+|~-=\`{}[:];'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered by you.

A password may contain several words, i.e. a passPHRASE: "My Secret @\$[Password!]"

## 7.5. Password Protection Standards

Do not use the same password for TwinNET accounts as for other non-TwinNET access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various site access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share TwinNET passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, *CONFIDENTIAL* information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- If someone demands a password, refer him or her to this document or have him or her call the local Account Administrator.
- Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger, Internet Explorer).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to the TwinNet Security Group and change all passwords.

#### **7.5.1.1. Application Development Standards**

Application developers must ensure their programs contain the following security precautions. Applications:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.
- Should be aware of and test authentication security in developed applications.

#### **7.5.1.2. Use of Passwords and Passphrases for Remote Access System-level Users**

Access to the TwinNET Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

#### **7.5.1.3. Passphrases**

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The\*?#>\*@TrafficOnThe101Was\*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

## **7.6. Enforcement**

The site's Database Manager should disable a user's accounts if the user do not follow the requirements in this policy and ensure that the user has no access to the federated database until it is proven that the user is in compliance to the said requirements..

## **8. Remote Access Policy**

### **8.1. Purpose**

The purpose of this policy is to define standards for connecting to TwinNET's network from any host. These standards are designed to minimize the potential exposure of TwinNET to damages, which may result from unauthorized use of TwinNET resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical TwinNET internal systems, etc.

### **8.2. Scope**

This policy applies to all TwinNET site's employees, contractors, vendors and agents with a TwinNET-owned or personally owned computer or workstation used to connect to the TwinNET network. This policy applies to remote access connections used to do work on behalf of

TwinNET, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

### **8.3. Policy**

#### **8.3.1. General**

It is the responsibility of TwinNET site's employees, contractors, vendors and agents with remote access privileges to TwinNET's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to TwinNET systems.

#### **8.3.2. Requirements**

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong passphrases. For information on creating a strong passphrase see the Password Policy.
2. At no time should any TwinNET site employee provide their login or email password to anyone, not even family members.
3. TwinNET site employees and contractors with remote access privileges must ensure that their TwinNET-owned or personal computer or workstation, which is remotely connected to TwinNET's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Routers for dedicated ISDN lines configured for access to the TwinNET network must meet minimum authentication requirements of CHAP.
5. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
6. Frame Relay must meet minimum authentication requirements of DLCI standards.
7. The site must approve non-standard hardware configurations, and the TwinNet Security Group must approve security configurations for access to hardware.

8. All hosts that are connected to TwinNET networks via remote access technologies must use the most up-to-date anti-virus software and anti spyware, this includes personal computers.
9. Personal equipment that is used to connect to TwinNET's networks must meet the requirements of site-owned equipment for remote access.
10. Organizations or individuals who wish to implement non-standard Remote Access solutions to the TwinNET production network must obtain prior approval from the TwinNet Security Group.

## 9. Router Security Policy

### 9.1. Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of TwinNET.

### 9.2. Scope

This policy pertains to all routers and switches connected to TwinNET's production networks. Routers and switches within internal, secured networks and not connected to TwinNET are not affected.

### 9.3. Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use TACACS+, certificates or preshared keys for all user authentications.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
  - a. IP directed broadcasts
  - b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
  - c. TCP small services
  - d. UDP small services except ping which will be allowed only through the IPSec tunnel.
  - e. All source routing
  - f. All web services running on router
4. Use corporate standardized SNMP community strings.
5. Access rules are to be added as business needs arise.
6. The router must be included in the corporate enterprise management system with a designated point of contact.
7. Each router must have the following statement posted in clear view:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

## **10. Server Security Policy**

### **10.1. Purpose**

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is used for and/or operated by TwinNET. Effective implementation of this policy will minimize unauthorized access to TwinNET's proprietary information and technology.

### **10.2. Scope**

This policy applies to server equipment used for, owned by or operated by TwinNET.

This policy is specifically for equipment on the internal TwinNET network.

### **10.3. Policy**

#### ***10.3.1. Ownership and Responsibilities***

Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the TwinNet Security Group.

Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the TwinNet Security Group.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

#### ***10.3.2. General Configuration Guidelines***

- Operating System configurations should be in accordance with approved guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- The database server shall only be able to communicate with the Internet through the IPSec tunnel.
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

#### **10.4. Monitoring**

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - All security related logs would be kept online for a minimum of 1 week.
  - Daily incremental tape backups will be retained for at least 1 month.
  - Weekly full tape backups of logs will be retained for at least 1 month.
  - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to the site's Point of Contact, which reports to the TwinNet Security Group. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host.

#### **10.5. Compliance**

- Audits will be performed on a regular basis by authorized organizations within TwinNET.
- The internal audit group or the TwinNet Security Group, in accordance with the chapter on auditing in this document, will manage audits. The TwinNet Security Group will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

#### **10.6. Enforcement**

A site not complying with the minimum-security requirements stated above may be cut off from TwinNET until the requirements have been met.

# **11. Virtual Private Network (VPN) Policy**

## **11.1. Purpose**

The purpose of this policy is to provide guidelines for remote access IPsec or SSL Virtual Private Network (VPN) connections to the TwinNET network.

## **11.2. Scope**

This policy applies to all GenomEUtwin researchers, employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the TwinNET network. This policy applies to implementations of VPN that are directed through an IPsec Concentrator.

## **11.3. Policy**

All communication between TwinNET sites will be made through VPN tunnel using IPsec or SSL using AES 128 bits encryption or better. This means that each site is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees etc. needed to comply with this policy.

Only ports necessary for database queries will be open inside the VPN tunnel.

## **11.4. Enforcement**

Any site found to have violated this policy might be subject to disciplinary action, up to and including termination of connection.

## **12. Wireless Communication Policy**

### **12.1. Purpose**

This policy prohibits access to TwinNET networks via wireless communication mechanisms.

### **12.2. Scope**

This policy covers all data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of TwinNET's internal networks. This includes any form of communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to TwinNET's networks do not fall under the purview of this policy.

### **12.3. Policy**

No wireless devices will be connected to any TwinNET devices.

### **12.4. Enforcement**

Any site found to have violated this policy might be subject to disciplinary action, up to and including termination of connection.

## **13. Breach of security policy**

### **13.1. Purpose**

This policy details which steps will be taken in case of a breach of security.

### **13.2. Scope**

This policy applies to all TwinNET sites.

### **13.3. Policy**

When the TwinNet Security Group is informed about a breach of security it will take steps in the following order:

1. Inquiry  
The TwinNet Security Group contacts the site to inform it of the breach and advises it on which steps must be taken to remedy the situation. A reasonable deadline is set by the TwinNet Security Group depending on the seriousness and degree of difficulty of the situation.
2. Counseling  
If the site needs help to remedy the situation, the TwinNet Security Group will provide counseling and some assistance.
3. Reminder  
If the site, after a reasonable time, still has not fixed the problem, the TwinNet Security Group will send a reminder with a short deadline.
4. First warning  
If the site still has not fixed the problem a warning will be issued. The warning should include this chapter and information that if the situation is not remedied immediately the site may be disconnected.  
The Ethics Core is informed of the situation and will inform the GenomEUtwin Steering Group of the situation.  
No new projects will be authorized until the problem is solved.
5. Second warning  
This warning is issued by the Ethics Core and is a final warning before disconnect.
6. Disconnect  
If the site still has not resolved the problem the Ethics Core will instruct the TwinNet Security Group to disconnect the offending site from TwinNet.  
This will be done in order to preserve the faith of the other sites to the security of TwinNET.

If a site has been disconnected, it may be reconnected after the original problem has been solved and the site has given proper insurances to the Ethics Core and the TwinNet Security Group that all steps have been taken to avoid a recurrence of this situation. .

### **13.4. Enforcement**

Any site found to have violated this policy might be subject to disciplinary action, up to and including termination of connection.