Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico

Security Policy

Version 1.3

18/07/2012

Executive Summary

Il documento fissa le normative cui attenersi per garantire la sicurezza e la riservatezza delle informazioni gestite dalla Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico (Fondazione) all'interno dei propri sistemi informatici.

Index

1 Politiche di sicurezza informatica della Fondazione

1.1 Introduzione

L'Unità Operativa Sistemi Informativi (UOSI) della Fondazione al fine di garantire la sicurezza e la riservatezza delle informazione gestite in azienda, l'integrità dei dati e dei sistemi e la disponibilità dei sistemi ha definito una policy di sicurezza conforme alle norme vigenti a cui devono adeguarsi tutti i sistemi connessi alla rete aziendale.

La sicurezza informatica ha il compito di definire la protezione delle informazioni e dei sistemi informatici da accessi non autorizzati, uso, diffusione, disgregazione, modifica o distruzione; si adopera quindi affinché vengano perseguiti i criteri di confidenzialità, integrità e disponibilità delle informazioni.

La information security è fondata su tre principi chiave:

- **Confidenzialità**: le informazioni devono poter essere viste, copiate o trasmesse a persone che sono autorizzate a compiere queste azioni e solo quando ve ne sia una reale necessità.
- **Integrità**: nella sicurezza informatica, l'integrità dei dati consiste nell'assunto che i dati non possano essere creati, modificati o distrutti senza che vi sia un'autorizzazione.
- **Disponibilità**: Il concetto di disponibilità dei dati ha il significato di avere disponibili e correttamente funzionanti, tanto i dati, quindi i sistemi in grado di processare le informazioni, quanto i mezzi per esercitare i controlli di autorizzazione su questi.

Il presente documento è conforme con tutte le normative vigenti in materia di sicurezza informatica ed in particolare con il Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali.

1.2 Rete Fondazione

La rete aziendale della Fondazione è costituita dagli strumenti informatici presenti all'interno dei palazzi di proprietà della Fondazione Policlinico (definiti nell'allegato A) di proprietà della Fondazione stessa e dagli strumenti collegati agli apparati di rete.

1.3 Assets

L'asset aziendale è composto dalle seguenti tipologie di sistemi informatici:

- **Postazioni di lavoro utenti**: computer collegati alla rete informatica.
- **Server**: computer che erogano servizi ad altre macchine. Condividono servizi quali la gestione di una LAN, lo scambio e la condivisione di files (file server), la gestione della posta elettronica (mail server), l'ospitare sit web (web server), la gestione di periferiche come le stampanti (print server), il backup dei dati (server raid).
- **Medicali**: macchine interfacciate a apparecchiature medicali connesse alla rete.

1.4 Naming convention

Le macchine devono avere un'opportuna naming convention che ne faciliti la localizzazione. Ogni caratteristica deve essere divisa da un meno (-). La naming convention è definita come segue:

1. Nome dell'edificio in cui è localizzata la macchina.
2. Reparto dell'edificio in cui la macchina è localizzata.
3. Ruolo della macchina.
4. Numero di matricola dell'asset aziendale nell'inventory aziendale.

Questa convenzione è applicabile tanto alle macchine server quanto a quelle client appartenente agli asset aziendali.

Per quanto riguarda invece macchine messe a disposizione da fornitori, come macchine destinate al controllo, acquisizione e trattamento di dati medicali ed interfacciate a strumenti si applicano le seguenti convenzioni:

1. Nome dell'edificio in cui è localizzata la macchina.
2. Reparto dell'edificio in cui la macchina è localizzata.
3. Ruolo della macchina.

La sigla che contraddistingue ogni edificio è illustrata nell'allegato A, così come la classificazione dei reparti e la sigla che identifica il ruolo della macchina.

2 Requisiti Security Sistemi interni e gestiti direttamente dalla Fondazione

2.1 Patch

Il livello di patch delle macchine deve essere possibilmente aggiornato al mese corrente. L'aggiornamento delle macchine deve essere controllato e posto in opera tramite il sistema centralizzato utilizzato dalla Fondazione Policlinico.

Le informazioni circa il sistema in uso internamente sono reperibili nell'allegato B.

2.2 Sistema AntiVirus

Le macchine devono essere dotate di antivirus aggiornato con cadenza almeno settimanale; deve essere previsto, qualora non sia possibile usare l'antivirus aziendale l'invio dei log di aggiornamento dell'antivirus installato per la verifica della compliance.

Se si utilizza un metodo per il controllo centralizzato dell'antivirus non aziendale (es. console) questa deve essere messa a disposizione degli addetti al controllo.

Le informazioni circa il sistema in uso internamente sono reperibili nell'allegato B.

2.3 Naming convention

Le macchine inserite nel dominio dovranno adottare le convenzioni aziendali riguardo il nome macchina.

2.4 Utenze

Gli utenti non possono essere amministratori della macchina e gli amministratori devono essere nominalmente identificabili. La password i amministratore generica (administrator o root) non deve essere mai utilizzata e deve essere consegnata in busta chiusa alla segreteria dell'UOSI. Si sottolinea che tale password sarà immediatamente cambiata e messa in cassaforte UOSI per eventuali emergenze.

2.5 Dominio

Tutte le macchine devono essere inserite nel dominio secondo la naming convention approvata.

2.6 Password

Tutte le password impostate sui sistemi dovranno essere conformi a quanto definito nella politica di gestione delle password che dovrà essere richiesta all'UOSI.

È prevista anche l'autenticazione tramite smart card, dove esplicitamente richiesto e consentito.

2.7 Account locali

Le macchine inserite nel dominio non devono permettere il login di amministratore locale della macchina.

2.8 Accesso ad internet

L'abilitazione alla posta esterna e ad Internet deve essere preceduta da regolare richiesta al Responsabile dei Sistemi Informativi (UOSI).

Il computer, qualora abilitato alla navigazione in Internet, costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa e pertanto è proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. Deve pertanto rispondere ai requisiti definiti dalla politica di utilizzo di internet che dovrà essere richiesta all'UOSI.

Non è possibile utilizzare modem per il collegamento alla rete ed è espressamente vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), l'utilizzo di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames). Anche in questo caso è opportuno richiedere all'UOSI la politica di utilizzo di un computer connesso alla rete interna della Fondazione.

2.9 Sistemi non basati su Microsoft Windows

Il livello di patching del sistema operativo deve essere aggiornato almeno con cadenza mensile, dove possibile.

A prescindere da questo, è comunque necessario che il sistema operativo sia comunque sottoposto ad un hardening preventivo, ovvero:

- rimuovere o disattivare tutti i servizi non strettamente necessari alle attività svolte dalla macchina;
- rimuovere tutti gli account utente non necessari;
- chiudere le porte di comunicazione non utilizzate dagli applicativi installati;
- applicare le security patch per il software installato sulla macchina.

Per un dettaglio più approfondito dei requisiti che la blindatura deve rispettare, occorre fare riferimento alla procedura di hardening definita dall'UOSI.

3 Requisiti security sistemi interni non gestiti direttamente dalla Fondazione

3.1 Patch

I sistemi devono avere le patch per la sicurezza aggiornate all'ultimo service pack disponibile e devono avere installate le patch critiche aggiornate almeno all'ultimo mese. Se questo non fosse possibile in tempi utili, il fornitore deve dimostrare di aver preso le precauzioni necessarie a contrastare i problemi derivanti dalla non applicazione delle patch dandone immediata comunicazione.

3.2 Antivirus

Le macchine devono essere dotate di antivirus aggiornato con cadenza almeno settimanale. Se si utilizza un metodo per il controllo centralizzato dell'antivirus non aziendale (es. console) ove possibile questa deve essere messa a disposizione degli addetti al controllo. L'antivirus sulle macchine deve poter essere aggiornato automaticamente mediante un processo temporizzato e i log con i dati dell'aggiornamento, quando non sia possibile un sistema di controllo centralizzato, deve essere inviato agli addetti al controllo via email.

3.3 Naming convention

Le macchine interne non gestite dovranno adottare la convenzione aziendale per quanto riguarda i nomi macchina, al fine di facilitare una migliore localizzazione. Qualora ciò non fosse possibile, il nome macchina deve essere comunque concordato con i Sistemi Informativi.

3.4 Account locali

Le utenze locali, se necessarie, devono avere password conformi a quanto definito nella politica di gestione delle password che dovrà essere richiesta all'UOSI. Le password devono essere cambiate periodicamente come previsto dalla normativa e dalla politica della Fondazione.

3.5 Accesso ad internet

L'accesso ad internet non è consentito.

3.6 Sistemi non basati su Microsoft Windows

Il livello di patching del sistema operativo deve essere aggiornato almeno con cadenza mensile, dove possibile. A prescindere da questo, è comunque necessario che il sistema operativo sia comunque sottoposto ad un hardening preventivo, ovvero:

- rimuovere o disattivare tutti i servizi non strettamente necessari alle attività svolte dalla macchina;
- rimuovere tutti gli account utente non necessari;
- chiudere le porte di comunicazione non utilizzate dagli applicativi installati;

- applicare le security patch per il software installato sulla macchina.

Per un dettaglio più approfondito dei requisiti che la blindatura deve rispettare, occorre fare riferimento alla procedura di hardening definita dall'UOSI.

4 Requisiti security sistemi esterni collegati alla rete

4.1 Patch

I sistemi devono avere le patch per la sicurezza aggiornate all'ultimo service pack e alle ultime hotfixes.

4.2 Sistema AntiVirus

Le macchine che si collegano per assistenza remota/manutenzione devono avere un sistema antivirus aggiornato a non più di due giorni.

4.3 Network

Gli ospiti devono essere assegnati ad una rete distinta da quella aziendale.

4.4 Accesso ad internet

I consulenti esterni non hanno accesso all'esterno se non tramite la rete guest completamente separata dalla rete interna di Fondazione.

4.5 Sistemi non basati su Microsoft Windows

Il livello di patching del sistema operativo deve essere aggiornato almeno con cadenza mensile, dove possibile.

A prescindere da questo, è comunque necessario che il sistema operativo sia comunque sottoposto ad un hardening preventivo, ovvero:

- rimuovere o disattivare tutti i servizi non strettamente necessari alle attività svolte dalla macchina;
- rimuovere tutti gli account utente non necessari;
- chiudere le porte di comunicazione non utilizzate dagli applicativi installati;
- applicare le security patch per il software installato sulla macchina.

Per un dettaglio più approfondito dei requisiti che la blindatura deve rispettare, occorre fare riferimento alla procedura di hardening definita dall'UOSI.

4.6 Disclosure Agreement Form

Tutti gli esterni collegati alla rete dovranno sottoscrivere un modulo (allegato C) in cui dichiarano di essere conformi ai requisiti indicati.

4.7 Eccezioni

La presente policy si intende applicata a tutti i sistemi, qualsiasi eccezione deve essere concordata con la direzione dei Sistemi Informativi.

5 Requisiti security sistemi per assistenza remota

5.1 Patch

I sistemi devono avere le patch per la sicurezza aggiornate all'ultimo service pack e alle ultime hotfixes.

5.2 Sistema AntiVirus

Le macchine che si collegano per assistenza remota/manutenzione devono avere un sistema antivirus aggiornato a non più di due giorni.

5.3 Accesso ad internet

I sistemi utilizzati per l'assistenza remota non hanno accesso alla rete interna. Non è consentito l'utilizzo di una doppia scheda di rete, una sulla rete interna ed una utilizzata verso l'esterno.

5.4 Sistemi non basati su Microsoft Windows

Il livello di patching del sistema operativo deve essere aggiornato almeno con cadenza mensile, dove possibile.

A prescindere da questo, è comunque necessario che il sistema operativo sia comunque sottoposto ad un hardening preventivo, ovvero:

- rimuovere o disattivare tutti i servizi non strettamente necessari alle attività svolte dalla macchina;
- rimuovere tutti gli account utente non necessari;
- chiudere le porte di comunicazione non utilizzate dagli applicativi installati;
- applicare le security patch per il software installato sulla macchina.

Per un dettaglio più approfondito dei requisiti che la blindatura deve rispettare, occorre fare riferimento alla procedura di hardening definita dall'UOSI.

5.5 Disclosure Agreement Form

Tutti gli esterni collegati alla rete dovranno sottoscrivere un modulo (allegato C) in cui dichiarano di essere conformi ai requisiti indicati.

5.6 Eccezioni

La presente policy si intende applicata a tutti i sistemi, qualsiasi eccezione deve essere concordata con la direzione dei Sistemi Informativi.

5.7 Allegato A

La rete del Policlinico è composta dai palazzi indicati nella seguente tabella.

Padiglione	Indirizzo	Sigla

5.8 Allegato B

- Il sistema AntiVirus attualmente in uso presso la Fondazione Policlinico di Milano è il **Symantec AntiVirus SEP 11**.

- Il sistema di centralizzazione dei log attualmente in uso presso la Fondazione Policlinico di Milano è il **Symantec SIM (Security Information Manager)**.

- Il sistema per l'aggiornamento delle patch di Microsoft attualmente in uso presso la Fondazione Policlinico di Milano è il **Microsoft Windows Server Updates Services (WSUS)**.

- I DNS interni di riferimento per la risoluzione dei nomi coincidono con i server Microsoft Active Directory 2003.

- Il sistema di riferimento per data e ora è l'NTP Microsoft presente sui server di dominio.

5.9 Allegato C

Io sottoscritto _____ ,

rappresentante dell'azienda_____ ,

presente all'interno della Fondazione Policlinico in data/nel periodo _____

_____ ,

DICHIARO

che le apparecchiature informatiche utilizzate all'interno della rete della Fondazione Policlinico sono conformi ai requisiti sottoindicati.

- Patch - I sistemi devono avere le patch per la sicurezza aggiornate all'ultimo service pack e alle ultime hotfixes.
- Sistema AntiVirus - Le macchine che si collegano per assistenza remota/manutenzione devono avere un sistema antivirus aggiornato a non più di due giorni.
- Network - Gli ospiti devono essere assegnati ad una rete distinta da quella aziendale.
- Accesso ad internet - I consulenti esterni non hanno accesso all'esterno se non tramite la rete guest completamente separata dalla rete interna. Il comportamento da tenere in navigazione è rigorosamente in linea con quanto letto sulla politica della Fondazione sull'utilizzo di internet.
- Il livello di patching del sistema operativo deve essere aggiornato almeno con cadenza mensile, dove possibile. A prescindere da questo, è comunque necessario che il sistema operativo sia comunque sottoposto ad un hardening preventivo, in linea con la procedura di blindatura consegnatami dalla Fondazione.
- Tutte le password utilizzate nel sistema rispettano le politiche definite dalla Fondazione che mi sono state consegnate.

Data

Firma