

# Regolamento per l'utilizzo delle risorse di Calcolo e Reti nella Sezione INFN di Bologna

*Franco Brasolin e Ombretta Pinazza*  
*Servizio di Calcolo e Reti*  
*Sezione INFN di Bologna*

# Caratteristiche del sistema informatico nella Sezione di Bologna

- grande numero di hosts
- eterogeneita' OS e HW
- numero elevato di utenti "esperti"
- autonomia acquisto e gestione macchine

Esigenza di un "regolamento" per garantire piu' sicurezza e responsabilizzare gli utenti

## I ruoli dei vari soggetti:

- > patrocinio Direzione
- > implementazione da parte del Servizio di tutti gli strumenti e misure per rafforzare la sicurezza informatica
- > adeguamento/collaborazione da parte degli utenti

# 1 - Patrocinio Direzione

La Direzione, preso atto del problema e sentiti i pareri del Servizio Calcolo e Reti, degli indirizzi dettati dal gruppo Security dell'I NFN, delle norme di legge vigenti, detta una serie di misure organizzative e comportamentali a cui devono attenersi tutti gli utenti, attraverso l'adozione di un *regolamento per la sicurezza informatica*.

## 2 - Realizzazione

Il personale del Servizio Calcolo e Reti, partendo dalle indicazioni dettate dalla Direzione, individua e installa gli strumenti più appropriati per raggiungere lo scopo e implementa le misure tecnologiche atte a rafforzare tali direttive.

## 3 - Utenti

- sono tenuti ad adeguare il proprio comportamento all'indirizzo politico della Sezione
- collaborano segnalando problemi o nuove necessità
- monitorano i sistemi che gestiscono
- segnalano al Servizio ogni sospetto di effrazione o violazione del regolamento

## Gli utenti devono essere informati e responsabilizzati

La Direzione ha incaricato il Servizio di fornire agli utenti le nozioni di base in materia di sicurezza informatica attraverso la redazione di note informative, pagine Web e l'organizzazione di corsi interni.

Un utente "informato" diventa responsabile delle sue azioni. Se l'utente non è sufficientemente informato, la responsabilità per le sue azioni può essere condivisa o fatta ricadere sul Responsabile del Servizio, sull'APA (responsabile amministrativo locale GARR-B) o sul Direttore di Sezione.

L'utente non informato, oltre a mettere in pericolo la propria postazione di lavoro, rappresenta un "buco" nella sicurezza dell'intero sistema informatico della Sezione e/o dell'Ente.

Per questi motivi, il Servizio, con il patrocinio della Direzione, richiede a tutti gli utenti dei sistemi informatici di Sezione l'accettazione scritta della politica di sicurezza informatica attraverso la firma di un modulo prestampato, con il quale si prende atto della responsabilità personale legata all'utilizzo di mezzi informatici .

# II Regolamento

<http://www.bo.infn.it/calcolo/policy/index.html>

- > Regole e principi generali per una politica di sicurezza informatica
- > Descrizione delle misure di sicurezza adottate
- > Elenco delle misure di sicurezza da implementare su tutte le macchine "private"
- > Dichiarazione di responsabilita' personale
- > Riferimenti normativi in materia di sicurezza informatica
- > Aggiornamenti





# 1. Regole di utilizzo delle risorse di Calcolo e Reti

- L'accesso e' personale e non cedibile; e' riservato a dipendenti, associati, dottorandi, laureandi, ospiti...
- Le risorse di calcolo e reti sono destinate alle attivita' istituzionali dell'Ente
- Sono vietate: attivita' commerciali, illegali, che violano la sicurezza e/o la privacy
- Ogni utente e' responsabile del software installato sulla propria macchina
- Tutti i gruppi/servizi nominano un referente che interfaccia gli utenti con il Servizio di Calcolo
- Ogni risorsa di calcolo e' affidata a un responsabile (utente/referente/Servizio di Calcolo)
- La responsabilita' dell'Account e' comunque personale e non puo' essere delegata



# 1. Regole di utilizzo delle risorse di calcolo e reti

## Il "Responsabile della risorsa di calcolo"

- Ogni utente deve firmare una "Dichiarazione di assunzione di responsabilita'" nella quale indica il responsabile delle risorse di calcolo
- Si assume la responsabilita' del corretto utilizzo e amministrazione della risorsa, nel rispetto del Regolamento, delle leggi sulla privacy, ecc.
- Risponde del software installato sul computer che gli e' affidato
- Interfaccia l'utente e il Servizio
- Il responsabile e il Servizio devono essere in grado in qualsiasi momento di accedere alle risorse di calcolo
- I responsabili devono consultare gli aggiornamenti, applicare gli antivirus e installare le patch di sicurezza

- **Regole di utilizzo delle risorse di calcolo e reti**  
**Le Responsabilita' degli utenti**

- L'accesso alle risorse di calcolo e reti e' personale, non va condiviso o ceduto
- Gli utenti devono proteggere i propri account mediante password
- Gli utenti sono responsabili per la protezione dei dati presenti/memorizzati nei sistemi in cui hanno accesso
- Gli utenti segnalino immediatamente ogni sospetto di incidente/abuso/effrazione/violazione della sicurezza

# 1. Regole di utilizzo delle risorse di calcolo e reti

## E' vietato:

- sono vietate le attività illegali
- sono vietate attività commerciali non previste dal contratto di lavoro
- sono vietate tutte le attività che compromettono in qualsiasi modo la sicurezza delle risorse di calcolo e reti
- sono vietate tutte le attività che possono rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software brevettato
- è vietato distribuire software soggetto a Copyright acquistato dall'Ente, al di fuori dei termini delle licenze
- è vietato distribuire software che possa danneggiare le risorse di calcolo, anche via e-mail
- è vietato accedere a dati e/o programmi per i quali non vi è autorizzazione o esplicito consenso da parte del proprietario



## E' vietato anche:

alcune di queste attivita' sono curate dal Servizio in maniera centralizzata per monitorare/controllare;  
vanno comunque sempre **AUTORIZZATE**

- utilizzare strumenti che potenzialmente sono in grado di consentire l'accesso non autorizzato alle risorse di calcolo (ad esempio cracker o software di monitoraggio della rete)
- configurare servizi già messi a disposizione in modo centralizzato, quali DNS, DHCP, NTP, mailing, accesso remoto
- aprire siti Web personali
- effettuare operazioni di routing, bridging, tunneling
- intercettare pacchetti sulla rete, utilizzare sniffer o software analoghi

## E' vietato inoltre:

- è vietato l'accesso ai locali del Servizio di Calcolo e Reti, ai locali e ai *box* riservati alle apparecchiature di rete, o apportare qualsiasi modifica agli stessi senza l'autorizzazione del Servizio
- è vietato cablare o collegare apparecchiature alle prese di rete senza l'autorizzazione del Servizio
- è vietato utilizzare indirizzi di rete e nomi non espressamente assegnati all'utente dal Servizio
- è vietato effettuare copie di file di configurazione del sistema
- è vietato installare modem configurati in call-back
- tutti gli accessi via modem devono essere autenticati e criptati
- è vietato divulgare i numeri telefonici e le password dei modem

## E' vietato infine (varie):

- è vietato intraprendere azioni allo scopo di:
  - degradare le risorse del sistema
  - impedire ad utenti autorizzati l'accesso alle risorse
  - ottenere risorse superiori a quelle già allocate ed autorizzate
  - accedere a risorse di calcolo, sia dell'Ente che di terze parti, violandone le misure di sicurezza

# Misure di sicurezza

## Principi generali

- Utilizzare accessi criptati
- Chiudere i servizi non essenziali e insicuri
- Monitor e Logging delle attività critiche del sistema
- Password "sicure", evitare di usare le stesse su sistemi diversi, cambiarle spesso
- Utilizzare programmi antivirus, applicare le patch di sicurezza, tenere aggiornati i sistemi
- E-mail: evitare di aprire messaggi da mittenti sconosciuti, diffondere virus alert e "catene di S.Antonio"



# Misure di sicurezza adottate dal Servizio di Calcolo e Reti sulle macchine di servizio

- Chiusura di servizi e programmi che trasmettono password in chiaro (telnet → **SSH**, FTP → **SCP** o **SFTP** ...)
- Revisione periodica degli account & **Cracker**
- Monitoraggio dei sistemi e della rete (**Swatch, Arpwatch, Tripwire**...)
- Filtraggio e logging delle porte sui router di accesso
- Installazioni centralizzate di sistemi (Linux/kickstart, W2000/RIS)

# Legislazione vigente

[Acceptable use policy della rete GARR](#), versione preliminare del 15 giugno 2000.

[Provvedimento](#) del Garante per la protezione dei dati personali sulle misure minime di sicurezza del 29 febbraio 2000.

[Decreto del Presidente della Repubblica 28 luglio 1999, n. 318](#) - Regolamento recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675.

[Decreto legislativo 22 maggio 1999, n. 185](#) - Attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza.

[Decreto legislativo 11 maggio 1999, n. 135](#) - Disposizioni integrative della legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte di soggetti pubblici.

[Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999](#) - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513.

[Decreto del Presidente della Repubblica 10 novembre 1997, n. 513](#) - "Regolamento contenente i criteri e le modalità di applicazione dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 in materia di formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici".

[Legge 31 dicembre 1996 n. 675](#) - "Tutela delle persone e di altri soggetti rispetto al trattamento di dati personali".

[Direttiva UE 95/46/CE del 24 ottobre 1995](#) - "Sulla protezione dei dati personali".

[Decreto del Presidente del Consiglio dei Ministri 3 gennaio 1994, n. 244](#) - "Regolamento concernente il registro pubblico speciale per i programmi per elaboratore".

[Legge 23 dicembre 1993 n. 547](#) - "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

[Decreto Legislativo 29 dicembre 1992 n. 518](#) - "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore".

# Cronologia

- giugno 2000: redazione del Regolamento
- luglio 2000: presentazione ufficiale agli utenti (congiunta Direzione/Servizio di Calcolo e Reti)
- ottobre 2000: check-list e corsi interni
- ottobre 2000: inizio richiesta moduli responsabilita'
- entro fine anno: a regime

# Reazioni degli utenti

- **reazione** tutto sommato positiva, buona presa di coscienza
- **richiesta di check-list** da seguire per mettere in sicurezza i propri sistemi
- **richiesta di corsi interni** relativi alla sicurezza e all'utilizzo di SW

## Reazioni del personale del Servizio

- carico di lavoro e responsabilita'
- difficolta' di integrazione/interazione con l'Universita'