R E G O L A M E N T O

per l'utilizzo delle risorse di Calcolo e Reti

del Dipartimento di Fisica - Università degli Studi di Perugia

---

N.B. : **Per gli ultimi aggiornamenti legislativi e delle normative interne dell'Ateneo**, si rimanda al relativo Portale, come da collegamenti seguenti:

- *Privacy e Sicurezza Informatica*: http://www.unipg.it/contenuti/newstory/privacySicurezza/
- *Linee guida per l'utilizzo della rete internet e della posta elettronica:* http://www.unipg.it/documenti/statutoRegolamenti/linee-guida-per-l-utilizzo-della-rete-internet-e-della-posta-elettronica.pdf
- *Codice in materia di protezione dei dati personali* (D.Lgs 196/2003 e successive modifiche): http://www.unipg.it/contenuti/newstory/privacySicurezza/DLvo196_30_06.pdf
- *Regole di uso per la Rete nazionale dell'Università e della Ricerca* (Consorzio GARR): http://www.net.unipg.it/node/39

Introduzione

Il **Servizio di Calcolo e Reti** (di seguito indicato anche come **Servizio**) si occupa della configurazione e dell'amministrazione delle risorse di calcolo e reti.
Per *risorse di calcolo e reti* si intendono:

- macchine del Servizio;
- workstation, personal computer, stampanti utilizzati da dipendenti, associati, dottorandi, laureandi, ospiti ecc. - servizi e/o esperimenti (anche condivisi con gli enti di ricerca convenzionati, INFM ed INFN);
- tutte le macchine facenti comunque parte della rete **fisica.unipg.it**;
- apparati di rete;
- tutto il software e i dati acquistati o prodotti per l'amministrazione dei sistemi, per l'utilizzo da parte degli utenti o di terzi autorizzati.

Motivazioni

Negli ultimi anni le risorse di calcolo all'interno del Dipartimento sono considerevolmente aumentate e con esse l'utilizzo della rete Internet. Tutto questo ha avuto importanti ricadute sui problemi di sicurezza, come confermano recenti episodi di intrusione. Si è reso quindi necessario attivare una serie di norme, restrizioni e controlli

per garantire la sicurezza dei sistemi e definire le responsabilità degli utilizzatori delle risorse.
L'adozione di queste politiche viene fatta nell'intento di:

- garantire la massima efficienza delle risorse di calcolo,
- garantire la riservatezza delle informazioni e dei dati,
- provvedere ad un servizio continuativo nell'interesse della comunità didattica e scientifica,
- provvedere ad un'efficiente attività di monitoraggio e controllo,
- garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche,
- garantire la massima sicurezza nell'interazione tra il Dipartimento e i centri di calcolo di altre istituzioni.

E' compito dell'Ente:

- adottare tutti i dispositivi di sicurezza necessari a difendere i propri sistemi informatici;
- implementare meccanismi di controllo e monitoraggio;
- responsabilizzare e formare gli utenti circa i rischi penali, civili, amministrativi connessi all'uso indebito dei mezzi informatici o alla riproduzione non autorizzata di *software*;
- evitare che i propri utenti, utilizzando gli strumenti di calcolo del Dipartimento, si introducano abusivamente in sistemi informatici, o che si verifichino casi di abusiva duplicazione e/o commercializzazione di programmi software.

SOMMARIO

Il presente **Regolamento** fornisce la descrizione delle regole da rispettare e dei comportamenti da adottare in materia di *sicurezza informatica*, ed è costituito dalle seguenti parti:

- **Introduzione generale** (il presente paragrafo);
- **Regole di utilizzo** delle risorse di calcolo e reti;
- **Misure minime di sicurezza** che devono essere rispettate da tutti gli utenti del Dipartimento, nonché altre necessarie misure preventivamente o eventualmente adottate dal Servizio;
- **Normativa essenziale** per gli utenti della rete locale;
- **Modulo di dichiarazione di assunzione delle responsabilità**, che ogni utente deve sottoscrivere, contenente l'accettazione integrale delle regole sull'utilizzo delle risorse di calcolo.
  Una clausola speciale riguarda gli *utenti privilegiati* che hanno pieno controllo dei propri computer (come *root* o *Administrator*): questi utenti dovranno assumersi formalmente la piena responsabilità della macchina, del software installato e del suo corretto utilizzo.

REGOLE DI UTILIZZO DELLE RISORSE DI CALCOLO E RETI

Premessa

- le seguenti regole devono essere seguite attentamente da tutti gli utenti;
- per quanto non specificato nei presenti documenti è richiesto comunque un atteggiamento ispirato alla correttezza ed alla buona fede;
- resta valida in ogni caso l'assunzione di responsabilità personale per la propria macchina;
- in caso di dubbi, necessità di informazioni, sospetto di tentativi di intrusione ecc. rivolgetevi immediatamente al Servizio di Calcolo e Reti.

Accesso alle risorse di calcolo e reti

- l'accesso alle risorse di calcolo e reti è riservato al personale docente e non docente del Dipartimento di Fisica, ai dipendenti INFN, , ai dipendenti INFM, ai collaboratori, agli ospiti; a dottorandi, specializzandi, assegnisti, borsisti e laureandi autorizzati dai relativi tutori;
- ogni risorsa di calcolo è affidata ad un ***utente***, che deve sottoscrivere la **dichiarazione di accettazione** delle politiche di sicurezza del Servizio; viene definito ***responsabile*** per la gestione e l'utilizzo della risorsa di calcolo:
    - l'utente, se questi ne richiede il controllo completo,
    - il referente delegato nel modulo di accettazione,
- il responsabile designato deve avere esperienza, capacità e affidabilità che garantiscano il pieno rispetto del presente regolamento;
- in ogni caso il Servizio si riserva il diritto ad accedere alla risorsa di calcolo per compiti di monitoraggio, controllo e/o aggiornamenti, ai fini della sicurezza del sistema e della rete, nel rispetto della presente politica di gestione e della riservatezza dei dati personali (ai sensi della **legge 675/96).**

Utilizzo delle risorse di calcolo e reti

- Le risorse di calcolo e reti della Dipartimento di Fisica di Perugia sono destinate alla ricerca scientifica e alla didattica e **possono essere utilizzate esclusivamente per le attività istituzionali**, salvo quanto previsto dal contratto nazionale di lavoro e dalla convenzione INFN – Università e INFM/CNR-Università.
- Sono comunque vietate:
    - attività commerciali non previste dal contratto di lavoro,

- tutte le attività che possono rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software brevettato,
- tutte le attività che compromettono in qualsiasi modo la sicurezza delle risorse di calcolo e reti,
- ovviamente, anche ogni altra attività illegale qui non elencata.

Responsabilità degli utenti

- l'accesso alle risorse di calcolo e reti è personale e non può essere condiviso o ceduto;
- gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso;
- gli utenti devono proteggere i propri account mediante ***password***;
- gli utenti sono obbligati a segnalare immediatamente al Servizio ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza**;**
- gli utenti sono tenuti a mantenersi aggiornati, controllando periodicamente le direttive del Servizio.

Software e copyright

- il responsabile risponde del software installato sul computer che gli è affidato;
- il responsabile provvede all'acquisto, o alla regolarizzazione, delle licenze necessarie per il software presente sul computer che gli è affidato;
- è vietato distribuire software soggetto a Copyright acquistato dal Dipartimento di Fisica, 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.

Le seguenti attività sono in generale vietate (sebbene nei termini consentiti possano essere svolte, a scopo di monitoraggio e per garantire la sicurezza esclusivamente dal Servizio o da personale preventivamente autorizzato, nel rispetto delle norme sulla riservatezza dei dati personali):

- 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 (Domain Name Service) mailing.
- intercettare pacchetti sulla rete, utilizzare *sniffer* o software analoghi.

Amministratori di sistema

- si definisce amministratore di sistema il soggetto a cui è conferito il compito di sovraintendere alle risorse del sistema operativo di un computer (**L. 318/99, art. 1, comma 1.c**)
- gli amministratori di sistema sono obbligati ad operare nel rispetto delle politiche del Dipartimento in materia di sicurezza, garantendo la massima riservatezza nella trattazione dei dati personali;
- il Servizio e/o gli amministratori di sistema si riservano il diritto di revocare l'accesso alle risorse di calcolo e di rete senza preavviso, qualora essi siano utilizzati impropriamente o in violazione delle leggi vigenti;
- è vietato installare software che possa compromettere il livello di sicurezza delle risorse di calcolo (in caso di dubbio consultare il Servizio);
- eventuali utilizzi abusivi delle risorse di calcolo devono essere immediatamente segnalati al Responsabile del Servizio di Calcolo e Reti;
- il personale del Servizio e/o i referenti locali devono essere in grado, in caso di emergenza, di poter accedere in qualsiasi momento ai locali e alle risorse di calcolo a loro affidati.

Inoltre (divieti generali)

- è assolutamente vietato l'accesso 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: in particolare, **ogni sostituzione o aggiunta di schede di rete deve essere preventivamente segnalata ai tecnici**, per la registrazione degli indirizzi ethernet univoci *(MAC address)*; così pure l'installazione di hub (anche piccoli) per sottoreti di calcolatori e stampanti nei gruppi di studio o di ricerca;
- è vietato utilizzare indirizzi di rete e nomi non espressamente assegnati all'utente dal Servizio;
- è vietato installare modem configurati in *call-back*;
- 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 del Dipartimento che di terze parti, violandone le misure di sicurezza;
    - accedere ai file di configurazione del sistema, farne delle copie e trasmetterle ad altri;
    - svelare le password altrui, nonché trasmettere in chiaro, pubblicare o mandare in stampa liste di account utenti o nomi host e corrispondenti indirizzi IP delle macchine.

Ogni azione che non sia comunque conforme allo spirito del presente Regolamento, verrà considerata una violazione della sicurezza, e come tale comporterà la revoca dell'accesso alle risorse di calcolo e rete, e la segnalazione al Responsabile. I casi più gravi verranno segnalati all'Autorità competente e potranno essere soggetti ad azioni disciplinari o legali.

Misure di sicurezza richieste agli utenti

Ecco un elenco di misure di sicurezza generali a cui tutti gli utenti sono tenuti ad attenersi. In caso di dubbi o per richieste di informazioni specifiche rivolgetevi al Servizio di Calcolo.

Misure generali:

- ogni computer è affidato ad un responsabile (che può essere il proprietario, il referente del servizio, o il Servizio di Calcolo e Reti) che si assume la responsabilità del corretto utilizzo e amministrazione della risorsa;
- la password di utente privilegiato deve essere nota al Servizio o al referente locale per gli interventi di amministrazione remota sulla macchina; l'utente che amministra personalmente come *root* o *Administrator* la propria macchina si assume tutte le responsabilità che questo comporta; in caso di necessità il Servizio ha il diritto comunque di richiedere l'accesso al sistema;
- il sistema deve essere mantenuto per quanto possibile sicuro: indicazioni sulla sicurezza del proprio sistema sono riportate qui di seguito, o possono essere ottenute dal personale del Servizio;
- il sistema deve essere monitorato; ogni sospetto di possibile intrusione e ogni altro problema di sicurezza vanno immediatamente segnalati al Servizio;
- ogni utente deve fare un uso appropriato della risorsa che gli è affidata. Nell'impossibilità di stabilire criteri di giudizio riguardo a questo argomento ci si affida al buon senso e al giudizio di ogni utente, il quale si è assunto la piena responsabilità delle sue azioni.

Consigli per la scelta della password

- la password deve avere almeno 7 caratteri ed essere composta da lettere maiuscole e minuscole, numeri e caratteri speciali . ? ^ % $ #
- evitare parole del dizionario (qualunque lingua!), nomi propri o geografici;
- cambiare regolarmente la password;
- evitare di usare la stessa password su sistemi diversi;
- non utilizzare procedure per l'accesso che contengano la password;
- non tenere le proprie password scritte su file o procedure.

Misure specifiche per tutti gli utenti

- gli utenti non devono comunicare a nessuno le proprie password né concedere ad altri l'uso del proprio account, del quale sono pienamente responsabili;
- gli utenti possono accedere alle risorse di calcolo remote utilizzando **SSH** (anziché **telnet**) e **SCP** (anziché **ftp**), che permettono di aprire sessioni remote o trasferire file trasmettendo le informazioni in formato criptato;
- non montare filesystem da una connessione remota;
- non utilizzare la propria password da connessioni remote non sicure;
- gli utenti sono invitati ad utilizzare programmi antivirus e a provvederne regolarmente all'aggiornamento;
- quando un computer rimane inutilizzato è consigliabile chiudere eventuali collegamenti remoti e impedire l'accesso alla console terminando la sessione corrente;
- al momento del login verificare la provenienza dell'ultima sessione di lavoro;
- evitare di utilizzare i file *.rhosts* e */etc/hosts.equiv*;
- evitare di utilizzare file o directory *world-writable;*
- utilizzare con cautela programmi gratuiti (o shareware) prelevati da siti Internet o in allegato a riviste o libri;
- se vengono utilizzati floppy disk (o similari), rispettare le seguenti prescrizioni:
    - sottoporre a scansione antivirus i dischetti di provenienza incerta, gia' adoperati in precedenza o preformattati;
    - proteggere in scrittura i dischetti di boot, di installazione o contenenti programmi eseguibili.

Misure specifiche per gli utenti privilegiati (root e Administrator)

- gli utenti privilegiati devono prestare particolare attenzione a:
    - limitare altri accessi privilegiati al proprio sistema,
    - evitare di collegarsi come root dall'esterno della rete di appartenenza,
    - utilizzare l'accesso ordinario per accedere ai propri file personali, limitando l'accesso privilegiato ad operazioni di amministrazione del sistema,
    - utilizzare l'accesso ordinario e il comando su per avere l'accesso privilegiato.
- gli utenti privilegiati sono tenuti a informarsi regolarmente riguardo le patch di sicurezza o gli aggiornamenti relativi al sistema operativo che gestiscono; il Servizio cercherà di dare il massimo supporto informativo;
- gli utenti privilegiati devono scegliere le proprie password con particolare attenzione, evitando di utilizzare la stessa password per diversi account e cambiandola regolarmente;
- gli utenti privilegiati sono tenuti a monitorare il proprio sistema tenendo sotto osservazione in particolare i seguenti aspetti:
    - tentativi di accesso falliti,

    - accessi come utente privilegiato,
    - programmi con il bit setuid,
    - file *.rhosts*,
    - modifiche ai file di sistema,
    - password troppo facili,
    - */var/adm/messages* o equivalenti,
    - activity log file (*history* o equivalenti);
- è vietato installare programmi di monitoraggio pacchetti (network snooping);
- è vietato installare programmi di intercettazione password (sniffing);
- per motivi di sicurezza evitare di usare programmi come IRC, ICQ o Napster essendo programmi potenzialmente pericolosi;
- è vietato aprire siti Web personali: il sito Web è gestito in modo centralizzato dal Servizio di Calcolo e Reti.

Misure di sicurezza specifiche per utilizzatori di Microsoft Windows

- come per altri sistemi operativi, evitare di utilizzare l'account di Amministratore, se non necessario;
- utilizzare possibilmente dei buoni programmi antivirus e mantenerli aggiornati;
- è assolutamente indispensabile eseguire dei back-up periodici dei dati sensibili;
- eseguire periodicamente le operazioni automatiche di aggiornamento Windows attivabili da *Start - Windows update,* o attraverso il sito ufficiale Microsoft (http://windowsupdate.microsoft.com/);
- installare, dove possibile, il software *Microsoft Windows critical update notification*, attivabile anch'esso dalle pagine Web di Microsoft;
- browser Internet Explorer:
    - disattivare l'opzione di completamento automatico (*strumenti - opzioni Internet - completamento automatico*) perché memorizza le password;
    - limitare al massimo possibile l'esecuzione automatica di *cookies* e *scripts* (ActiveX, Java, ...) in: *strumenti - opzioni Internet - Security – Custom;* scegliere quali eseguire e quali rifiutare
- Posta elettronica:
    - impostare il browser di posta in modo da mostrare solo le intestazioni dei messaggi, senza aprirli automaticamente;
    - evitare di aprire eventuali allegati *.VBS (Visual Basic Script) ai messaggi di posta, quando provengano da mittenti poco sicuri o sconosciuti: se possibile, disattivare l’esecuzione automatica di ogni file *.vbs tramite programmi di soglia, oppure analizzarli prima con un buon software antivirus aggiornato;
    - non diffondere mai messaggi di tipo “allarme-Virus!” o altre catene di Sant'Antonio (vengono iniziate da malintenzionati a scopo di creare intasamento nelle reti,

oppure di procurarsi quantità di indirizzi e-mail da bombardare successivamente con pubblicità commerciale indesiderata - il cosiddetto *spamming*: per la stessa ragione, evitare pure di rispondere a messaggi che invitano a farlo per annullare la propria (mai avvenuta) iscrizione ad una lista (sono un trucco operato da terzi per crearsi un database di indirizzi sicuramente attivi di posta elettronica, da bersagliare poi con lo *spamming*)

Per la generalità dei browser:

- riguardo ai *cookies*, se sono necessari (ad es., per login a secure webmailer) attivare se possibile soltanto quelli che danno una semplice risposta al server.

Normativa essenziale

Sono riportate solo informazioni rilevanti per amministratori di sistema e per utenti del Dipartimento di Fisica di Perugia: il presente quadro non intende essere esaustivo di tutta la Normativa in vigore.

1. **Legislazione vigente**
2. **Reati penali**
3. **Illeciti civili**
4. **Sanzioni amministrative** (un esempio)

---

1 - Legislazione vigente

N.B. : **Per gli ultimi aggiornamenti legislativi e delle normative interne dell'Ateneo**, si rimanda al relativo Portale, come da collegamenti seguenti:

- *Privacy e Sicurezza Informatica*: http://www.unipg.it/contenuti/newstory/privacySicurezza/
- *Linee guida per l'utilizzo della rete internet e della posta elettronica:* http://www.unipg.it/documenti/statutoRegolamenti/linee-guida-per-l-utilizzo-della-rete-internet-e-della-posta-elettronica.pdf
- *Codice in materia di protezione dei dati personali* (D.Lgs 196/2003 e successive modifiche): http://www.unipg.it/contenuti/newstory/privacySicurezza/DLvo196_30_06.pdf
- *Regole di uso per la Rete nazionale dell'Università e della Ricerca* (Consorzio GARR): http://www.net.unipg.it/node/39

2 - Reati penali

In questa breve sintesi sono elencate alcune figure di reato previste dal **Codice Penale** (**legge 547/93**, pene variabili fino ad un massimo di cinque anni di reclusione):

- Attentato a impianti informatici di pubblica utilità (art. 420);
- Falsificazione di documenti informatici (art. 491bis);
- Accesso abusivo ad un sistema informatico o telematico (art. 615ter);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615quater);
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615quinquies);
- Violazione di corrispondenza telematica (artt. 616-617sexies);
- Intercettazione di e-mail (art. 617quater);
- Danneggiamento di sistemi informatici e telematici (art. 635bis);
- Frode informatica (alterazione dell'integrità di dati allo scopo di procurarsi un ingiusto profitto) (art. 640ter).

Protezione dei sistemi informatici da attacchi esterni

Le aziende (**DPR 318/1999**, **Legge 675/96**) dovranno adottare tutti i dispositivi di sicurezza necessari (parole-chiave, codici logici ecc.), per difendere i propri sistemi informatici da attacchi esterni. Ciò non solo per opportuna prevenzione ma anche per consentire l'eventuale incriminazione del soggetto attivo, con la conseguente richiesta di danni in sede civile.
Dovranno anche essere posti in atto tutti gli interventi necessari a ridurre i rischi di coinvolgimento dell'azienda, nell'ipotesi che i reati sopra elencati siano commessi dai propri dipendenti che, utilizzando gli strumenti aziendali, si introducano abusivamente nei sistemi informatici di terzi.
Ferma la responsabilità dell'autore del comportamento illecito, il nostro ordinamento penale prevede infatti la categoria dei cosiddetti "reati omissivi impropri" (**art. 40 cpv c.p.**) che si concretizzano nella violazione di un generico obbligo giuridico di impedire determinati eventi dannosi.
E' previsto anche il coinvolgimento penale del datore di lavoro, a titolo di concorso nel reato commesso da un proprio dipendente, nella misura in cui le circostanze concrete dimostrino che il comportamento criminoso del dipendente sia stato agevolato dalla mancata adozione, da parte del datore di lavoro, di idonee misure di prevenzione e controllo (anche in materia di abusiva duplicazione e/o commercializzazione di programmi per elaboratore).

"Obblighi di controllo" del datore di lavoro

Il Garante per la protezione dei dati personali ha emesso, il 29/2/2000, un provvedimento, allo scopo di richiamare l'attenzione dei soggetti pubblici e privati tenuti al rispetto del **DPR 318/99** (obbligo di predisporre misure minime per la sicurezza) sulle prescrizioni in

esso contenute e sulle connesse sanzioni, nonché sulla scadenza del 29/3/2000 prevista per l'applicazione delle misure minime di sicurezza. Nell'ottobre 1999 anche **l'AIPA** (Autorità per l'Informatica nella Pubblica Amministrazione) ha pubblicato le "Linee guida per la definizione di un piano per la sicurezza".
Cautele minime la cui adozione potrebbe fortemente limitare i rischi di un coinvolgimento penale del datore di lavoro:

- Responsabilizzazione degli utilizzatori finali, attraverso la diffusione dell'informazione circa i rischi penali connessi all'uso indebito del mezzo informatico o alla riproduzione non autorizzata di software.
- Formazione degli utilizzatori finali, attraverso corsi di introduzione e di aggiornamento, non solo mirati all'aspetto tecnico-applicativo, ma anche alla tematica della sicurezza informatica.
- Limitazione degli accessi a sistemi informatici esterni solo agli utilizzatori che ne abbiano effettiva necessità per ragioni di servizio, adottando le misure idonee per vigilare su comportamenti potenzialmente dannosi del dipendente.
- Meccanismi di controllo dei vari personal computer per verificare l'esistenza di software non autorizzato.

"Datore di lavoro" e delega di funzioni

Le eventuali responsabilità penali derivanti dalla commissione dei "reati informatici" potrebbero essere assunte da un **"Delegato alla sicurezza informatica"** purché la delega risulti da atto scritto e sia accettata dal delegato, soggetto tecnicamente competente, qualificato e idoneo allo svolgimento dei compiti assegnatigli.
L'ipotesi di reato a carico del responsabile della sicurezza è "Omessa adozione di misure necessarie alla sicurezza dei dati" (**art.36 L. 675/96**): "Chiunque, essendovi tenuto, omette di adottare le misure necessarie ad assicurare la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti [...], è punito con la reclusione fino ad un anno. Se dal fatto deriva nocumento, la pena è della reclusione da due mesi a due anni".

---

3 - Illeciti civili

Devono essere adottate le cautele minime che chiunque, dotato di un livello di diligenza media in relazione alle circostanze e alla competenza professionale, avrebbe adottato, tenuto conto delle migliori tecniche messe a disposizione dallo sviluppo tecnologico del settore.

Misure di sicurezza

Principi di massima ai quali ispirare una politica aziendale di sicurezza informatica:

- Rispetto dei requisiti di "diligenza professionale", richiesti dall'articolo 2050 del codice civile.
- Adeguamento preventivo ai contenuti espressi dall'art. 15 della legge 675/96 (Legge sulla *privacy*).
- Adeguamento sostanziale alle "Linee Guida per la definizione di un piano per la sicurezza", a cura dell’AIPA (http://www.aipa.it)

- Allineamento a standard riconosciuti a livello comunitario o internazionale (es. ITSEC: http://www.aipa.it/attività/progettiintersettoriali/sicurezza/itsec/)

---

4 - Sanzioni amministrative (un esempio)

Attenzione a non diffondere messaggi di posta elettronica di tipo *"catena di S. Antonio"* o contenente messaggi pubblicitari indesiderati! **In base all'Articolo 10 del DLgs 185/99 l'**invio di ***messaggi di posta elettronica*** *non sollecitati* costituisce una violazione punibile con sanzione amministrativa pecuniaria.

Dichiarazione di assunzione di responsabilità
(modello di)

Prima di firmare leggere attentamente il documento allegato:
Regolamento per l'utilizzo delle risorse di Calcolo e Reti - Dipartimento di Fisica dell'Università di Perugia.

Il sottoscritto, firmando il presente documento, riconosce di aver letto, compreso ed accettato integralmente le politiche e le regole del Dipartimento di Fisica dell'Università degli Studi di Perugia, riguardo l'utilizzo e l'accesso alle risorse di Calcolo e Reti; il sottoscritto si assume inoltre la piena responsabilità in caso di violazione delle leggi e dei regolamenti riconducibili al suo accesso personale e/o alle risorse di calcolo sottoelencate:

Nome e Cognome :
……
Indirizzo e-mail :
……
Ente di appartenenza :
……
Data : ……

Firma : ……

Nomino come **Responsabile** delle seguenti risorse di calcolo:
.....
.....
.....
.....
.....

- ☐ **me stesso** (sono in possesso della password di accesso privilegiato)
- ☐ **il Referente** …… (è in possesso della password di accesso privilegiato)
- ☐ **il Servizio di Calcolo** (è in possesso della password di accesso privilegiato)

(barrare una sola voce)

Firma dell' Utente richiedente:

……

Firma del Responsabile :

……