

REGOLAMENTO RELATIVO ALL'UTILIZZO DEI MEZZI INFORMATICI E TELEMATICI DEL DTI

- Articolo 1 Scopo e validità
 - Articolo 2 Definizioni
 - Articolo 3 Competenze e responsabilità
 - Articolo 4 Concetto
 - Articolo 5 Misure di sicurezza
 - Articolo 6 Condizioni e scopi dell'utilizzo
 - Articolo 7 Presenza in rete
 - Articolo 8 Riserva relativa al diritto superiore
 - Articolo 9 Responsabilità
 - Articolo 10 Definizione di abuso
 - Articolo 11 Notifica
 - Articolo 12 Sanzioni
 - Articolo 13 Entrata in vigore
-

La direzione del DTI,

basandosi sulle responsabilità che gli derivano nella gestione del Dipartimento, delle sue attrezzature e dei suoi servizi stabilisce:

Articolo 1 Scopo e validità

Questo regolamento ha l'obiettivo di indicare a tutti gli utenti dei mezzi telematici del DTI quali sono gli utilizzi possibili degli stessi; in particolar modo rispetto ai concetti di sicurezza e considerando il principio che essi devono servire, in condizioni ottimali, agli scopi generali del DTI.

Articolo 2 Definizioni

1. Per mezzi telematici (risorse) s'intendono le apparecchiature, le attrezzature, i servizi che vengono impiegati per l'elaborazione elettronica di dati, come hardware, software, reti, dati, documentazione, consulenza e formazione.
2. Per utilizzo s'intende qualsiasi uso dei mezzi telematici.
3. Per servizi informatici si intendono le risorse di persone e attrezzature destinate, esplicitamente in organigramma, alla gestione dei sistemi informatici e telematici del DTI (compiti e definizione di questo servizio sono resi espliciti al di fuori di questo regolamento).
4. Per utenti si intendono i collaboratori del DTI (docenti, ricercatori, personale amministrativo, personale tecnico o qualsiasi altra persona che offre prestazioni lavorative), gli studenti del DTI o in generale della SUPSI e terze persone che potrebbero essere autorizzate all'uso.

Articolo 3 Competenze e responsabilità

1. I servizi informatici del DTI sono responsabili, oltre che del generico supporto agli utenti e la gestione ordinaria e straordinaria dei sistemi informatici e telematici (come stabilito dalle regole di gestione del dipartimento), anche della sicurezza dei sistemi telematici del DTI.
2. In particolare i servizi informatici sono competenti per:
 - a) la protezione dei sistemi informatici e delle applicazioni informatiche;

- b) l'accertamento, le prove documentate e l'eliminazione di difetti di sicurezza;
 - c) la coordinazione e il controllo delle misure di sicurezza;
 - d) provvedimenti tecnici relativi alla sicurezza telematica, comprendenti prove documentate e la rimozione di difetti tecnici;
 - e) la tenuta di un inventario relativo alle applicazioni in caso di particolari necessità di protezione (vedi allegati);
3. La direzione del DTI ha la competenza di comminare sanzioni in caso di abusi (art. 12).

Articolo 4 Concetto

Il concetto di sicurezza, prima di essere implementato, viene progettato e documentato dai servizi informatici, sottoposto per approvazione dalla direzione del DTI e reso noto (dove l'informazione non sia in contrasto con il concetto stesso) agli utenti che ne facciano esplicita richiesta.

Articolo 5 Misure di sicurezza

1. Per applicazioni o sistemi con necessità di protezione devono essere utilizzate delle password. La password è legata alla persona; non può essere ceduta a terzi, né resa accessibile, inoltre è consigliabile una frequente ridefinizione della stessa.
2. L'attrezzatura e l'utilizzo di accesso diretto alla rete di comunicazione, necessitano di un'autorizzazione scritta da parte dei servizi informatici. Esempi di attività non permesse sono:
 1. Il collegamento di elaboratori senza il consenso esplicito dei servizi informatici.
 2. Il cambiamento non autorizzato dei parametri relativi alla connessione (p.es. il numero IP).
 3. L'asportazione o l'aggiunta di parti di hardware non esplicitamente approvato.
 4. L'installazione di software che possa provocare danno ai sistemi interni o esterni.

Articolo 6 Condizioni e scopi dell'utilizzo

1. I mezzi telematici propri del DTI possono essere utilizzati per adempiere agli obiettivi generali del DTI. Fanno eccezione le applicazioni che necessitano di una specifica autorizzazione.
2. L'utilizzo per l'apprendimento e la ricerca è prioritario a qualsiasi altro impiego.
3. Il prestito, l'affitto e la vendita di mezzi telematici sono ammessi unicamente previa autorizzazione scritta della direzione del DTI e comunicazione ai servizi informatici.
4. Un utilizzo commerciale è consentito solo con un permesso scritto della direzione del DTI, la quale stabilisce inoltre il relativo prezzo.
5. La pubblicità commerciale è proibita. Eventuali eccezioni sottostanno alla decisione della direzione.
6. Non sono consentite forme di utilizzo per scopi privati o comunque non inerenti alle attività del dipartimento o della SUPSI che carichino in maniera eccessiva il sistema informatico e telematico o che provochino danno ad altri utenti, tra cui la distribuzione di messaggi di posta elettronica, allegati, files o documenti in "broadcast" a tutta l'utenza.
7. L'elaborazione di dati personali è permessa esclusivamente nell'ambito degli scopi generali del DTI e deve essere conforme alla legislazione sulla protezione dei dati.
8. L'uso per altri scopi (personali) è tollerato se:
 - provoca costi trascurabili,
 - non contrasta con gli interessi e l'immagine del DTI,
 - non ostacola l'accesso ad altri utenti autorizzati,

Articolo 7 Presenza in rete

1. Per l'immagine del DTI nella rete mondiale e interna (ma estesa alla SUPSI) è responsabile la direzione generale della SUPSI.
2. A tale scopo la direzione generale stabilisce le necessarie regole e in particolare quali pagine di accesso devono essere create in modo uniforme.
3. Per le pagine interne alla rete DTI è responsabile la direzione del DTI
4. A tale scopo la direzione del DTI, se necessario, stabilisce le regole.
5. In ogni caso sulle pagine Web nella rete mondiale, di tutte le unità figura: il responsabile e il realizzatore della pagina, e la data di pubblicazione. Il responsabile è colui che si assume completamente la responsabilità di quanto viene pubblicato sulla rete, che in molti casi corrisponde con il realizzatore.

6. Le pagine Web devono essere aggiornate.

Articolo 8 Riserva relativa al diritto superiore

1. Viene applicato il diritto nazionale e internazionale vigente in Svizzera.
2. In modo particolare devono essere rispettate le condizioni di licenza, le leggi relative ai beni immateriali e specialmente i diritti d'autore di terzi, come pure la protezione dei dati.

Articolo 9 Responsabilità

1. Gli utilizzatori sono in linea di principio personalmente responsabili per l'utilizzo di mezzi telematici (attrezzature e dati).
2. In caso di utilizzo per adempiere a mandati di diritto pubblico, particolarmente tramite collaboratori DTI, vale la legge relativa alla responsabilità.
3. Salvo un'esplicita assicurazione scritta degli organi competenti, il DTI non si assume responsabilità per difetti tecnici dei mezzi telematici e per le loro conseguenze.

Articolo 10 Definizione di abuso

1. Un utilizzo illegale di mezzi telematici, ossia che non rispetta le citate norme, che non corrisponde agli obiettivi generali del DTI, che è sproporzionato, o per il quale non c'è la necessaria autorizzazione, può essere punito.
2. In modo particolare, è considerato abuso un accesso non autorizzato ai mezzi telematici, come pure la violazione di leggi relative a licenze e altri beni immateriali e la violazione della protezione dei dati.
3. Un utilizzo dei mezzi telematici inconciliabile con gli interessi del DTI è considerato un grave abuso. Ne fanno parte dati con contenuti razzistici o pornografici.

Articolo 11 Notifica

Si fa obbligo a docenti e altri collaboratori del DTI d'annunciare al/agli addetto/i ai sistemi eventuali utilizzi abusivi, o illegali, di cui vengono a conoscenza.

Articolo 12 Sanzioni

1. La direzione del DTI può, a chi abusa di mezzi telematici, prendere provvedimenti quali un ammonimento, il blocco dell'accesso, la cancellazione dei dati, altra limitazione o il divieto dell'utilizzo. In aggiunta possono essere inoltrati procedimenti disciplinari, o civili, oppure può essere sporta denuncia.
2. Casi particolarmente gravi possono portare all'annullamento dell'immatricolazione, o al licenziamento.
3. In caso di sospetto fondato di abuso la direzione del DTI può preventivamente bloccare l'accesso. Essa deve provvedere affinché i dati in questione siano ricercati e conservati.
4. Il DTI può addebitare costi derivanti da abusi a chi li ha causati.

Articolo 13 Entrata in vigore

Il presente regolamento entra in vigore retroattivamente dal 1° gennaio 2000.

Per la direzione DTI

Giambattista Ravano
direttore

ALLEGATO: MISURE DI PROTEZIONE PER SISTEMI TELEMATICI

1. Utilizzo con bassa necessità di protezione (categoria default)

1. Utilizzi che non fanno parte di alcuna categoria d'alta protezione, rientrano nella categoria default, per cui una bassa protezione è sufficiente.
2. Gli utilizzatori sono personalmente responsabili delle seguenti misure di sicurezza:
 - a) Adeguata copia di sicurezza dei dati a scadenza regolare;
 - b) Immediata comunicazione ai servizi informatici di problemi di sicurezza come difficoltà, difetti, abusi, violazioni delle condizioni d'uso;
 - c) Collaborazione nel controllo;
 - d) Eventuale installazione e attivazione dei più recenti software anti-virus.

2. Utilizzo con alta necessità di protezione

1. Nell'inventario viene elencato:
 - a) La descrizione delle applicazioni;
 - b) L'ubicazione del server;
 - c) Il/la responsabile del sistema;
 - d) La lista degli utilizzatori;
 - e) Le misure di sicurezza, che superano le misure di sicurezza della categoria default, come pure le successive misure di sicurezza obbligatorie già citate.
2. Il responsabile di sistema deve provvedere all'attuazione delle alte misure di sicurezza seguenti:
 - a) Identificazione dell'utilizzatore;
 - b) Protezione della password con controllo regolare;
 - c) Log-out in caso d'abbandono del posto di lavoro;
 - d) Immediata comunicazione di problemi di sicurezza;
 - e) Periodico controllo tramite gli addetti alla sicurezza;
 - f) Redazione di un piano per la sicurezza dei dati;
 - g) Designazione del/della sostituto/a del/della responsabile del sistema.
3. I responsabili del sistema possono stabilire per singole applicazioni le seguenti addizionali misure di sicurezza:
 - a) limitazione d'accesso fisico;
 - b) protezione dei dati a mezzo di
 1. cifratura di trasmissione dati (Public Key Infrastructure);
 2. firma digitale
 3. identificazione degli indirizzi di utilizzatori finali;
 4. protezione router
 5. Firewall
 - c) Strategie alternative in caso di prolungato ammanco del sistema.