DOCUMENTO PRESCRITTIVO DEL DPS

Allegato n. 10 del:

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

(Misure di sicurezza per il trattamento di dati personali, art. da 33 a 36 del Decreto Legislativo 30/06/2003 n. 196)

Revisione		
Indice	**Data**	**Motivo della revisione**
Revisione: 0	20/03/2006	I emissione in ottemperanza al D. lgs. 30/06/04 n. 196: Rev. 0Data: 20/03/2006
Rev.:1	30/03/2007	Revisione in sede di bilancio consuntivo anno 2007
Rev.: 2	15/06/2009	Revisione in ottemperanza alla applicazione della normativa sugli amministratori di sistema
Rev.: 3	15/12/2009	Revisione per modifica Allegati
Revisione 4	16/03/2011	Revisione contenuto
Revisione 5 (corrente)	08/03/2012	Revisione e modifica Allegati

Classificazione del documento**: pubblico**

SOMMARIO

1 - Obiettivi

Il presente documento, allegato e parte integrante del Documento Programmatico sulla Sicurezza del Dipartimento di Statistica, definisce le regole comportamentali e le responsabilità connesse alle misure di sicurezza: in particolare con l'obiettivo di garantire i requisiti e definire la manutenzione delle procedure. Esso fornisce indicazioni atte a:

- garantire la sicurezza dei dati ai sensi del D.lgs.vo 30.6.2003 n.196 (recante il Codice in materia di protezione dei dati personali) e il suo Disciplinare Tecnico (Allegato B);
- assicurare l'adempimento delle "Misure Minime" di sicurezza previste nel Disciplinare Tecnico;
- operare in modo da seguire le "Misure Idonee" a preservare i dati, in relazione ai rischi ai quali sono sottoposti.

Nel presente documento vengono fornite indicazioni per garantire la sicurezza nei suoi vari aspetti (riservatezza, integrità, disponibilità) attraverso misure di tipo logico e procedurale.

2 - Definizioni

Definizioni utili ai fini della applicazione del documento:

- **dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- "**dati sensibili**", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- "**trattamento**", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- "**titolare**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo **cui competono**, anche unitamente ad altro titolare**, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali** e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- "**responsabile**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo **preposti** dal titolare al **trattamento di dati personali**;
- "**incaricati**", le persone fisiche autorizzate a **compiere operazioni di trattamento** dal titolare o dal responsabile, se designato;
- "**Sistema informatico**", server di rete o computer personale;

- "**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- "**credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- "**parola chiave**", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- "**profilo di autorizzazione**", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- **"dati strategici"** per il Dipartimento di Statistica, i dati relativi ai servizi considerati strategici per le finalità e le attività svolte dal Dipartimento di Statistica;

- 'Decreto': il Decreto Legislativo 30.6.2003 n.196;
- "Regolamento di Ateneo": Decreto rettorale, 29 dicembre 2005, n. 1177 (prot. n. 79382), Bollettino Ufficiale Anno IV, Supplemento II al N. 12 - Dicembre 2005
- "Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici" (allegato A4 G.U. n. 190 del 14 agosto 2004)
- "GARR Acceptable Use Policy (AUP) ", Acceptable Use Policy della rete GARR

In base al "Regolamento di Ateneo" il Dipartimento di Statistica nella persona del Direttore è Responsabile di tutti i dati da esso detenuti, fatta eccezione per i dati, i programmi e i contenuti:

a) delle pagine WEB individuali del personale del Dipartimento, inclusi database e link di qualsivoglia natura e comunque con le limitazioni previste dal regolamento interno di gestione del sito Web istituzionale
b) dati memorizzati in rete nelle aree di file services quali: home personali degli utenti, aree di rete condivise, aree di rete per il backup dei dati presenti nelle stazioni di lavoro personali
c) delle caselle di posta sul server, per il contenuto delle quali la responsabilità è del proprietario.

3 - Campo di applicazione

Le regole comportamentali definite nella presente procedura sono orientate alla protezione dei dati personali, sensibili e strategici, compresi quelli detenuti dal personale docente e ricercatore del dipartimento nell'ambito della propria attività di ricerca

Esse hanno la seguente applicabilità:

Sono **prescrizioni obbligatorie** ai sensi del D.lgs.vo 30.6.2003 n.196 per tutti coloro che trattano dati dei quali il Dipartimento di Statistica è titolare, in particolare per: gli **"incaricati speciali del trattamento**", cioè gli incaricati del Dipartimento di Statistica, con una o più delle funzioni di:

- **incaricato del trattamento;**
- **incaricato della custodia delle credenziali;**
- **incaricati della amministrazione di sistema, database e applicazioni**;

Sono regole di accesso e di comportamento per:

- tutto il personale afferente al Dipartimento di Statistica,
- tutti coloro che hanno rapporti di collaborazione con il Dipartimento di Statistica a qualunque titolo
- gli utenti della rete del Dipartimento di Statistica.

Si sottolinea che:

- chiunque intraprende trattamento di dati personali è tenuto a comunicarlo al Direttore del Dipartimento di Statistica, che ai sensi del "Regolamento di Ateneo"[1] è Responsabile del Trattamento dei dati del Dipartimento di Statistica;
- ciascuno ha la responsabilità dei dati detenuti sulla propria stazione di lavoro e della loro protezione; la condivisione dei dati sulle stazioni di lavoro personali deve essere ristretta alle sole persone incaricate di trattare tali dati e deve essere conforme alle norme di sicurezza;
- le caselle di posta elettronica possono contenere, oltre a dati propri, anche dati di altri ed in quanto tali, devono essere tutelate, anche sulle stazioni di lavoro personali.

Le regole comportamentali relative all'utilizzo delle apparecchiature di lavoro valgono per :

- stazioni di lavoro personali nel luogo di lavoro;
- stazioni di lavoro comuni a più persone, nel luogo di lavoro;
- stazioni di lavoro portatili;
- stazioni di lavoro dalle quali ci si connette in modalità remota;
- stampanti.

I Responsabili e gli Incaricati sono inoltre tenuti a quanto altro specificato nella nomina o anche successivamente indicato dal Responsabile del Trattamento e/o dai rispettivi Responsabili.

4 - Gestione degli accessi

Chiunque tratti dati informatici, sia sulla propria stazione personale che sui server di rete, deve essere abilitato e poi riconosciuto dal sistema informatico, cioè autenticato tramite delle **credenziali di autenticazione**; possono anche essere definiti a livello applicativo diversi "**profili di autorizzazione**", a seconda delle operazioni consentite a ciascuno degli incaricati del trattamento dei dati. Tipicamente le credenziali sono composte da:

- un identificativo dell'utente (*User ID*), che è la parte pubblica delle credenziali;
- una parola chiave di autenticazione (*password*), che è la parte riservata delle credenziali.

La *password* è un elemento fondamentale per il sicuro funzionamento del sistema di autenticazione e per evitare accessi non autorizzati. La scelta ed il corretto utilizzo delle password da parte dell'utente è dunque un fattore fondamentale per la sicurezza di un sistema informatico.

[1] Decreto del Rettore, 7 Luglio 2004, n. 449

4.1 - Modalità di scelta della password

Per garantire e mantenere l'efficacia delle misure di sicurezza, gli utenti devono essere consapevoli delle loro specifiche responsabilità nella **scelta delle password di accesso.** Affinché questa sia dotata di robustezza e quindi difficilmente intuibile da altri, è **obbligatorio** attenersi alle seguenti regole:

- la password deve essere composta da almeno otto caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la password non deve contenere riferimenti aventi attinenza con la vita privata o professionale facilmente riconducibili all'utente (evitare ad es. nome, cognome, data di nascita, numero di telefono, codice fiscale, luogo di nascita, nome di parenti ecc.);
- le password non devono essere parole di senso comune presenti sul dizionario;
- la password non deve contenere una serie consecutiva di soli numeri o di sole lettere;
- la password, nel caso in cui lo strumento elettronico lo permetta, deve essere preferibilmente composta da una sequenza di lettere, numeri e caratteri speciali (es. di caratteri speciali: &;@ *§ ? % £=@ $);
- la password non deve essere costituita da una sequenza ovvia sulla tastiera (es. qwerty, 12345678);
- la stessa password non deve essere riutilizzata per almeno quattro anni;
- la password deve essere facile da ricordare per l'utente, ad esempio formata dalle iniziali di una frase mnemonica.

4.2 - Cautele per la segretezza della password

Per garantire e mantenere l'efficacia delle misure di sicurezza, gli utenti **devono essere consapevoli** delle loro specifiche responsabilità nell'**utilizzo delle password di accesso**.

Nell'**utilizzo della password** devono quindi essere adottate le seguenti misure di sicurezza:

- utilizzare sempre esclusivamente le proprie credenziali di autenticazione;
- non condividere la propria password con altre persone;
- non comunicare ad altri le proprie credenziali;
- mantenere e custodire le proprie *password* con la dovuta riservatezza**;**
- evitare di scrivere le proprie *password* su foglietti di carta o agende, a meno che tali supporti cartacei non vengano custoditi in cassetti o armadi chiusi a chiave; nel digitare sulla tastiera la password, prestare attenzione ad eventuali sguardi indiscreti che potrebbero far perdere alla password di accesso il requisito della segretezza
- comunicare immediatamente al Responsabile la perdita della qualità delle credenziali in modo che siano subito disattivate.

4.3 - Obblighi relativi alla modifica della password

Per garantire e mantenere l'efficacia delle misure di sicurezza, gli utenti devono essere consapevoli delle loro specifiche responsabilità nella **modifica delle password di accesso**.

Per la **modifica della password** devono essere adottate le seguenti misure di sicurezza:

- modificare la password temporanea assegnata dall'amministratore, al primo utilizzo (primo logon);
- cambiare immediatamente la password nel caso si sospetti abbia perso il requisito della segretezza;
- modificare la password di accesso alle applicazioni utilizzate per il trattamento di dati personali almeno ogni sei mesi;
- **in caso di trattamento di dati sensibili** (es. dati personali inerenti lo stato di salute) e giudiziari **la password deve essere modificata almeno ogni tre mesi** (art.5 – Disciplinare tecnico -dal D.lgs. 196/2004);
- gli incaricati speciali del trattamento dati personali, sensibili, giudiziari o il responsabile, in caso di assenza di tali figure, devono comunicare all'incaricato della custodia delle credenziali la modifica, consegnandogli in busta chiusa le proprie credenziali (identificativo di utente e password).

5 – Gestione delle credenziali

Le credenziali di accesso ai sistemi sono distinte in:

1. credenziali di accesso alla rete del Dipartimento e alle risorse hardware e software della rete del dipartimento, gestite dal Laboratorio di Statistica
2. credenziali di amministrazione della propria stazione di lavoro (USERID administrator del sistema locale ed eventuale password del bios)
3. credenziali di accesso agli archivi e al software presenti nella propria stazione di lavoro.
4. credenziali di accesso alle applicazioni disponibili in Internet e gestite da strutture diverse dal Laboratorio di Statistica.

Credenziali di cui al punto 1: a ciascun utente della rete interna del Dipartimento viene assegnata la credenziale di autenticazione nella rete.
Sono previste le tipologie di utenza descritte in tabella 1
Possono essere assegnate ulteriori credenziali in funzione dei servizi ai quali l'utente ha accesso (es. posta elettronica).
Ulteriori differenziazioni all'accesso alle risorse di rete sono attribuite alle stazioni locali di lavoro in funzione della sottorete a cui sono connesse.
La credenziale attribuita all'utente è personale; l'utente è responsabile della corretta gestione come specificato nel paragrafo 4 del presente documento.
In caso di smarrimento, il personale tecnico accede alle procedure previste per resettare la password al valore iniziale.

Tabella 1 – Tipologie di utenza nella rete interna del Dipartimento

Codice	Descrizione	Durata	Area personale sui server di rete	Accesso ad Internet
1	Studenti del Corso di Laurea in Statistica	triennale	no	sì
2	Studenti dei Corsi di Laurea Specialistica "Statistica e Informatica per l'Azienda" e "Popolazione e Società"	biennale	no	sì
3	Tesisti di laurea con relatore afferente al Dipartimento di Statistica:	biennale	si	sì
4	Collaboratori esterni a ricerca con sede il Dipartimento di Statistica	temporanea	si	sì
5	Studenti il cui docente è afferente al Dipartimento di Statistica:	annuale	no	sì
6	Studenti dei corsi di dottorato con sede al Dipartimento di Statistica:	triennale	si	sì
10	Docenti e ricercatori	sino alla cessazione del servizio	si	sì
11	Ricercatori (non più utilizzato dall'1/1/2009)	sino alla cessazione del servizio	si	sì
12	personale tecnico	sino alla cessazione del servizio	si	sì
13	docenti altri dipartimenti/facoltà	annuale	si	sì
14	personale amministrativo	sino alla cessazione del servizio	si	
20	associazioni	annuale	no	si
21	codici generici per la didattica	Scadenza illimitata	no	no[2]
22	codici per interviste	Scadenza illimitata	si	sì
23	ospiti	temporanea	si	sì

L'attribuzione delle credenziali è disciplinate come segue:

- A tutto il personale docente e non docente, strutturato e non, in servizio o afferente al Dipartimento di Statistica viene attribuito un codice di accesso alla rete interna che

[2] Il codice Lezione ha l'accesso ad internet. Viene utilizzato nel caso di Lezioni in aula rivolte a personale esterno all'università di Firenze. Ha password con scadenza al termine della lezione. Viene utilizzato in base al regolamento interno

consente di usufruire delle risorse della rete stessa; tale codice scade con la cessazione del diritto di usufruirne da parte dell'utente.
- Per le tipologie 1-6 è prevista la compilazione di una richiesta su modulo cartaceo (allegato1) da parte dello studente che deve essere completata anche dal docente presentatore nel caso delle tipologie 3-6.
- Su richiesta di un docente del dipartimento di Statistica, qualificato come Responsabile, vengono definite aree in rete ad accesso condiviso. La richiesta deve essere eseguita compilando apposito modulo (allegato 4)

Al momento della creazione di un nuovo login di accesso alla rete, vengono assegnate ad ogni utente le proprie credenziali date da un codice di autenticazione e da una password iniziale standard. Tale password deve essere personalizzata dall'utente al primo accesso alla rete.
La password assegnata inizialmente viene anche utilizzata come password di ripristino in caso di dimenticanza di quella personale in uso.
La richiesta di ripristino della password iniziale deve essere fatta compilando l'apposito modulo (allegato 3: modulo di richiesta di servizi aggiuntivi al codice di utenza)

Il responsabile di trattamento di dati personali, sensibili, giudiziari deve consegnare in busta chiusa all'incaricato della custodia delle credenziali, le credenziali (USERID e password) di accesso a tali archivi.
Con riferimento alle credenziali di cui al punto 4, e cioè credenziali di accesso alle applicazioni disponibili in Internet e gestite da strutture diverse dal Laboratorio di Statistica, dovranno essere seguite le istruzioni impartite dall'ente o struttura che ha rilasciato le credenziali. Nel caso delle credenziali attribuite dall'amministrazione universitaria per l'accesso agli archivi della contabilità, delle presenze, ecc. dovranno essere applicate le disposizioni previste nel documento prescrittivo del DPS dello CSIAF

6 - Gestione delle stazioni di lavoro

Dato che la stazione di lavoro è il punto di accesso ai dati, particolare cautela deve essere adottata sia nella sua custodia che nella sua manutenzione operativa atta a prevenire virus informatici ed intromissioni, da parte di tutto il personale, strutturato e non, del Dipartimento

Nel caso poi che nella stazione di lavoro siano presenti archivi contenenti dati personali, sensibili e giudiziari, il responsabile di tali archivi dovrà seguire le istruzioni a lui impartite con la lettera di nomina a responsabile.

6.1 - Custodia della stazione di lavoro

Le presenti regole si applicano alle stazioni di lavoro registrate nell'inventario del Dipartimento di Statistica e alle stazioni di lavoro non in carico al Dipartimento di Statistica nel caso di autorizzazione all'accesso alla rete del Dipartimento.
Per garantire e mantenere l'efficacia delle misure di sicurezza, gli utenti devono essere consapevoli delle loro specifiche responsabilità nella **custodia della propria stazione di lavoro.**

Le informazioni riservate (dati personali, dati sensibili, dati strategici), necessitano di una

protezione più elevata e di particolare cautele da parte del personale incaricato del trattamento.

In ogni caso considerando che sulla propria stazione di lavoro sono presenti rubriche personali di indirizzi di posta elettronica e considerando che, ai sensi dell'art. 10 del "Regolamento di attuazione del codice di protezione dei dati personali in possesso dell'Università degli Studi di Firenze solo gli indirizzi della sede di lavoro del personale di Ateneo possono essere considerati "dati personali diffondibili incondizionatamente", tutti gli altri indirizzi non possono essere considerati diffondibili e perciò devono essere protetti alla stregua dei dati personali. Pertanto il personale è tenuto a seguire le seguenti istruzioni:

- evitare di lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- proteggere la stazione di lavoro attraverso cui si accede a sessioni di trattamento di informazioni riservate, utilizzando o key locks, password di qualità o screen saver (da attivare su richiesta o dopo un tempo prestabilito di inattività), nel caso in cui ci si assenti temporaneamente dall'ufficio;
- al termine della sessione di lavoro sui server centrali, effettuare la procedura di disconnessione ("log-off" / "logout") ;
- al termine della sessione sulla stazione di lavoro, effettuare la procedura di arresto del sistema ed attendere che sia terminata prima di lasciare l'ufficio;
- effettuare (almeno una volta alla settimana) il backup dei dati personali e documenti essenziali presenti sulla propria stazione di lavoro o portatile tramite il servizio di file service fornito dal Laboratorio o, ove impossibile, su CD.

6.2 - Prevenzione dei virus informatici

E' necessario prevenire l'introduzione di virus informatici che possano compromettere l'integrità del software e delle stazioni di lavoro, tenendo anche conto del fatto che tra un aggiornamento del programma antivirus ed il successivo è presente una finestra temporale di rischio di introdurre virus non ancora noti dal programma antivirus stesso.

E' necessario pertanto:

- installare il software antivirus in dotazione al Laboratorio di Statistica;
- configurare la protezione permanente e l'aggiornamento automatico via rete;
- verificare il regolare funzionamento della procedura automatica di aggiornamento del programma antivirus, al fine di accertarsi che la procedura sia andata a buon fine;
- utilizzare il software rispettando le istruzioni del fornitore;
- verificare, tramite adeguato programma antivirus, i file, il software e i dispositivi magnetici (floppy disk) provenienti dall'esterno, prima del loro utilizzo;
- configurare il sistema operativo affinché sia possibile visualizzare l'estensione dei file: tale accorgimento rende più difficile il mascheramento da parte di file potenzialmente pericolosi (programmi EXE e script di vario tipo) che impiegano estensioni doppie (es. "leggimi.txt.vbs" oppure "logo.jpg.exe");
- ripulire immediatamente le stazioni che si rivelino o vengano segnalate come infette;

- segnalare tempestivamente al Responsabile dei Servizi Informatici di Polo qualsiasi presenza di virus sospetta che pregiudichi o abbia pregiudicato il sistema di sicurezza delle informazioni;
- nello scaricare dalla rete *Internet* programmi (es. software open source; freeware, shareware ecc.) e documenti (testi e tabelle che possono contenere dei "*virus macro*") necessari allo svolgimento della propria attività lavorativa, utilizzare unicamente i siti delle case produttrici dei medesimi o i link che esse stesse propongono sul loro sito;
- nell'utilizzo della posta elettronica :
    - evitare di aprire allegati che contengono un'estensione doppia o con estensione VBS, SHS, PIF, EXE, COM o BAT (a meno che non attesi e provenienti da mittente conosciuto e di fiducia);
    - se si ricevono e-mail non richieste o con contenuti pubblicitari, evitare di seguire i collegamenti a indirizzi Web eventualmente presenti nel testo delle e-mail;
    - nel caso si riceva un messaggio di e-mail da una persona conosciuta, ma con un contenuto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato; infatti alcuni virus sono in grado di trasmettere messaggi con allegati che sembrano spediti da mittenti conosciuti;
    - evitare di cliccare su icone dall'apparenza innocua che ricordano applicazioni associate ad immagini o musica, mostrate dagli allegati di posta elettronica in quanto possono nascondere "*worm*"
    - configurare il programma di posta elettronica in modo tale che non esegua automaticamente gli allegati.
    - disattivare l'apertura automatica dei link in browser internet.

6.3 - Politica di aggiornamenti software

E' necessario prevenire, sulla propria stazione di lavoro, accessi non autorizzati che violino il sistema e possano compromettere l'integrità del software ed indirettamente dei sistemi informativi.

E' pertanto necessario seguire una politica di aggiornamento dei software presenti sulla stazioni di lavoro in modo da introdurre regolarmente le modifiche o le nuove versioni emesse per proteggere i sistemi. Adottare quindi le seguenti norme:

- configurare, ove possibile, l'esecuzione automatica degli aggiornamenti del sistema operativo, ovvero
- configurare, ove possibile, lo scaricamento automatico dalla rete degli aggiornamenti (patch) del sistema operativo ed eseguirne l'installazione non appena disponibile; ove non possibile un aggiornamento automatico, controllare almeno mensilmente la disponibilità di aggiornamenti e provvedere alla loro installazione;
- segnalare tempestivamente al Responsabile dei Servizi Informatici di Polo qualsiasi vulnerabilità o attività sospetta che pregiudichi o abbia pregiudicato il sistema di sicurezza delle informazioni.

6.4 – Aree Personali sui server della rete locale

Gli spazi dischi personali degli utenti e quelli ad accesso condiviso, presenti sui server di rete del Dipartimento di Statistica, sono considerati una estensione delle stazioni di lavoro personali o di ufficio.
Gli utenti e i Responsabili, nel caso di aree ad accesso condiviso, sono responsabili del contenuto, dell'accesso e della protezione dei dati.
Il contenuto delle cartelle:

- deve essere inerente alle attività istituzionali svolte dall'utente (o del gruppo di utenti per le Cartelle Condivise);
- deve essere conforme alla "Acceptable Use Policy (AUP)" della rete GARR;
- deve rispettare la normativa vigente e in particolare la tutela del diritto d'autore;
- deve essere privo di archivi di dati sensibili, per i quali non e' garantita la opportuna sicurezza.

La struttura Laboratorio di Statistica, cui è affidato il compito di gestione delle risorse informatiche, è responsabile della gestione degli utenti e profili di accesso, della sicurezza del server e dei salvataggi.
La richiesta di area ad accesso condiviso deve essere effettuata compilando l'apposito modulo (allegato 4)

7 - Aree WWW del Dipartimento di Statistica

L' area web, per sua natura, contiene dati a diffusione illimitata. In conseguenza il contenuto del sito web:

- deve essere privo di archivi di dati soggetti alla tutela della privacy
- deve essere inerente alle attività istituzionali svolte dal Dipartimento
- deve essere conforme alla "Acceptable Use Policy (AUP)" della rete GARR;
- deve rispettare la normativa vigente e in particolare la tutela del diritto d'autore;

La richiesta di assegnazione di spazio sul sito web del Dipartimento di Statistica o comunque sui server web gestiti dal Laboratorio di Statistica, da parte del personale autorizzato, per la propria homepage o per le attività istituzionali deve essere fatta su apposito modulo (allegato 2)

8 - Dati di log dei sistemi

I sistemi informatici e gli applicativi dedicati al funzionamento della rete dipartimentale, nel corso del loro normale funzionamento, registrano informazioni, la cui trasmissione è implicita nell''uso dei protocolli di comunicazione, non associate a Utenti direttamente identificabili.
Questi dati possono essere trattati al fine di controllare il regolare funzionamento della rete e per ricavare informazioni statistiche anonime sull'uso delle risorse tecnologiche.
I dati di Log soggetti alla normativa sulla privacy vengono raccolti su di un unico sistema a ciò preposto (log server), al quale hanno accesso solo gli incaricati a ciò adibiti; tali dati vengono via via archiviati su supporto magnetico e conservati per un periodo di 12 mesi; i dati potranno essere acquisiti esclusivamente su richiesta giudiziaria da parte di un pubblico ministero, secondo quanto previsto dalla normativa.

9 - Gestione del materiale

La sicurezza dei dati deve essere garantita anche quando non risiede su server e stazioni di lavoro.

In particolare deve essere protetto il materiale ottenuto come output da apparecchiature informatiche e non, ed il materiale cartaceo.

9.1 - Gestione del materiale di output

Per quanto riguarda il materiale ottenuto come output da apparecchiature informatiche e non, devono essere seguite le seguenti regole:

- se non utilizzati e quando ci si assenta dall'ufficio, provvedere a custodire in armadio o cassetto muniti di serratura i supporti removibili (es. floppy, cd) contenenti informazioni riservate o strategiche;
- controllare attentamente lo stato delle stampe di documenti riservati e rimuovere immediatamente tali copie dalla stampante, onde evitare che personale non autorizzato abbia accesso alle informazioni;
- provvedere a rendere inintelligibili eventuali stampe non andate a buon fine, anche utilizzando la trituratrice di documenti disponibile in Segreteria

9.2 - Gestione del materiale cartaceo

Per quanto riguarda il materiale cartaceo, devono essere seguite le seguenti regole:

- conservare i supporti cartacei contenenti dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati stessi (stanze, armadi, cassetti chiusi a chiave);
- se si è in attesa di un documento contenente informazioni riservate via fax, non lasciare incustodito l'apparecchio del fax ma rimuovere immediatamente il documento.

9.3 - Gestione delle apparecchiature dismesse

Le informazioni classificate come "riservate" (dati personali, dati sensibili ecc.) devono essere cancellate in maniera definitiva dai dispositivi di memorizzazione, prima che le apparecchiature vengano dismesse, o trasferite per essere riutilizzate da altri utenti, o consegnate al fornitore per riparazioni. Il semplice comando di formattazione non è spesso sufficiente per garantire una cancellazione permanente dei dati. Sono infatti disponibili diversi modi per recuperare i documenti che sono stati cancellati, anche dopo la formattazione dell'hard disk. Occorre prestare particolare attenzione quando si gestiscono *dati personali e sensibili*, *informazioni strategiche o coperte da riservatezza.* Per quanto concerne le vecchie stazioni di lavoro da eliminare, è compito di ciascun assegnatario provvedere alla permanente distruzione delle informazioni critiche e alla disinstallazione del software con licenza installato sulle stazioni di lavoro.

1) nel caso di reimpiego o di riciclo la cancellazione sicura può essere effettuata tramite
   - uno dei programmi di 'wiping' disponibili in rete (per es. DBAN, che si può scaricare dal sito http://www.dban.org, dove è disponibile anche la documentazione),
   - una formattazione a basso livello,
   - demagnetizzazione, che garantisce la demagnetizzazione anche per dispositivi non più funzionanti;

2) nel caso di smaltimento la cancellazione può anche prevedere la distruzione dei supporti tramite
   - sistemi di punzonatura o deformazione meccanica,
   - distruzione fisica o disintegrazione,
   - demagnetizzazione ad alta intensità.

Per quanto riguarda invece i server, gli storage system, le cartucce, in gestione al Laboratorio di Statistica (struttura interna del Dipartimento di Statistica) è compito di quest'ultimo di provvedere alla cancellazione permanente delle informazioni riservate. Per garantire l'impossibilità di recupero dei dati, si utilizzano tecniche di formattazione profonda, oppure si provvede alla distruzione fisica dell'apparecchiatura, dopo aver completato la procedura di scarico del bene inventariale.

10 - Allegati

allegato n.1: modulo per la richiesta/modifica della credenziale di accesso ai servizi disponibili sulla rete interna del Dipartimento di Statistica

allegato n.2: modulo per la richiesta di pubblicazione sul server web del Dipartimento di Statistica.

allegato n. 3: modulo di richiesta di servizi aggiuntivi al codice di utenza (ripristino della password iniziale, accredito ulteriori pagine di stampa, posta elettronica su ds.unifi.it)

allegato n. 4: modulo di richiesta di aree condivise

allegato n. 5: fac-simile richiesta attivazione banche dati contenente dati personali

allegato n. 6: Richiesta di inserimento dei computer nella rete del dipartimento