Al Sig.

OGGETTO: Conferimento incarico di Amministratore di sistema per il trattamento dei dati personali

Ai sensi e per gli effetti del provvedimento del Garante per la protezione dei dati personali dd. 27 novembre 2008 così come modificato dal provvedimento dd. 25/6/2009, il sottoscritto

, in qualità di responsabile della struttura dell'Università degli Studi di Trieste di seguito specificata:

TIPOLOGIA	DENOMINAZIONE
Amministrazione centrale	
Facoltà	
Dipartimento	
Centro autonomo di servizio	

nominato dal titolare quale responsabile del trattamento di dati personali svolto presso la struttura di riferimento

CONFERISCE

al Sig.

,

l'incarico con di Amministratore di Sistema, limitatamente al tempo di vigenza del rapporto in essere con l'Ateneo, limitatamente al seguente ambito:

nome applicativo/sistema informatico:

Di seguito si riportano alcune delle particolarità che caratterizzano tale incarico, per quanto di competenza dell'Università:

- é possessore dei codici e delle password di accesso per la configurazione del server e l'accesso alle funzioni sistemistiche e *dell'applicativo(ove ricorra)*;
- è incaricato di garantire l'efficienza e la disponibilità dei sistemi informativi di propria competenza;
- è incaricato di mantenere aggiornata la documentazione tecnica relativa alla configurazione software ed in particolare le procedure di attivazione e disattivazione del servizio, accensione e spegnimento del/i server coinvolti;
- è incaricato di garantire gli aggiornamenti periodici dei programmi volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti.

Istruzioni particolari impartite agli amministratori di sistema

- Nell'esecuzione dell'incarico, dovrà attenersi con la massima diligenza alle competenze e istruzioni descritte nel "documento programmatico per la sicurezza informatica" (D.P.S.) dell'Università, approvato con Decreto Rettorale n. 37760 dd. 23.12.2005 e soggetto a revisione annuale, da compiersi entro il 31 marzo, come disposto dalla normativa vigente.
- Mettere in atto le misure di sicurezza riportate nel DPS e quelle previste da leggi e norme vigenti in materia; più in generale, assicurare che l'utilizzo delle risorse informatiche e telematiche e delle banche dati elettroniche dell'Università avvenga con un adeguato livello di sicurezza e privacy;
- Assicurare la possibilità di accedere tempestivamente ai dati in situazioni di emergenza, secondo quanto prescritto dall'art. 10 del Disciplinare Tecnico del D.Lgs. 196/2003; a tale scopo è tenuto a consegnare al Custode delle Password, nella figura del responsabile del trattamento, un documento in formato cartaceo contenente l'elenco delle User ID e delle password associate a tutti i profili di tipo "Administrator" relativamente a tutti gli applicativi e ai sistemi operativi utilizzati;
- Identificare e segnalare al Titolare e ai Responsabili del trattamento dei dati casistiche di utilizzo non conforme alla normativa vigente e al Documento Programmatico sulla Sicurezza; in particolare accertare costantemente che gli incaricati utilizzino la parola chiave con diligenza e che la modifichino ogni qualvolta sussista il dubbio che essa sia stata manomessa.
- Assumere l'obbligo di eseguire periodicamente i controlli per verificare regolarmente l'efficienza, l'efficacia e la validità delle misure di sicurezza adottate;
- Assumere il compito di individuare e rimuovere o segnalare periodicamente (almeno ogni tre mesi) la presenza di vulnerabilità applicative presenti negli applicativi gestionali, che possono compromettere anche parzialmente la sicurezza dei dati e l'operatività dei programmi applicativi, dopo aver verificato che tali operazioni non compromettano la funzionalità di altri applicativi, su autorizzazione del Responsabile.
- Assicurare un supporto attivo, in base al ruolo ricoperto all'interno dell'organizzazione e per le competenze tecniche, nel coadiuvare il Responsabile e il Titolare nell'individuazione di puntuali istruzioni operative, attinenti all'applicazione delle misure minime ed idonee di sicurezza per il trattamento dei dati personali compiute attraverso strumenti elettronici, a specificazione e chiarimento di quelle generali impartite dai singoli responsabili, nonché il coordinamento dei relativi adempimenti riguardanti le procedure di autenticazione e autorizzazione, assieme all'assistenza in questo campo ai responsabili e agli incaricati del trattamento.
- Generare, sostituire ed invalidare, laddove previsto, in relazione agli strumenti e alle applicazioni informatiche utilizzate e secondo le misure di sicurezza, le parole chiave ed i codici identificativi personali da assegnare agli incaricati del trattamento dei dati personali.
- Adottare e verificare costantemente il corretto funzionamento di programmi antivirus e strumenti, sia software che hardware, che garantiscano - anche in relazione alle conoscenze acquisite in base al progresso tecnico - la sicurezza nel trattamento dei dati personali segnalando tempestivamente e per iscritto ai Responsabili dei trattamenti coinvolti,
- Segnalare per iscritto al responsabile
    1. l'individuazione di eventuali problemi;
    2. l'impossibilita' di adottare le misure minime o idonee previste, indicandone le motivazioni e le possibili soluzioni;

3. gli ulteriori criteri di sicurezza da adottare sia organizzativi che fisici, ferma restando la responsabilità del titolare nell'assicurare i mezzi e le risorse finanziarie per gli adeguamenti reputati necessari.

- Individuare, unitamente al responsabile del trattamento dei dati, le modalità e le procedure di reimpiego dei supporti di memorizzazione logica e, se del caso, individuare gli strumenti e le procedure adeguate per procedere alla distruzione e smaltimento dei supporti di memorizzazione che non possono essere riutilizzati.
- Definire, concordandole con i responsabili dei trattamenti coinvolti, procedure per la custodia di copie di sicurezza, prevedendo il salvataggio di copie almeno mensili in luogo diverso dall'edificio in cui risiedono i sistemi, nonché per il ripristino della disponibilità dei dati e dei sistemi.
- Prestare attenzione, per quanto di competenza, al fine di impedire l'accesso di estranei ai locali dove sono ospitati i server, anche in collaborazione con l'addetto alla sicurezza fisica dei locali ove si svolge il trattamento.
- Astenersi dal compiere attività di trattamento che comportino un accesso ed una conoscenza di informazioni superiore rispetto all'ambito di trattamento dei dati attribuito.
- Mettere in atto le procedure richieste dal Provvedimento del Garante della Privacy del 27/11/2008 relativamente alla registrazione degli accessi ai sistemi da parte degli amministratori di sistema o altri incaricati con profili privilegiati (Amministratori di rete, di applicativo o di database), mediante l'adozione di sistemi di access log che devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richiesti.

Trieste,

Firma del Responsabile del trattamento

Firma dell'Incaricato per ricevuta e presa visione: