ALLEGATO D

ISTRUZIONE PER LA GESTIONE DI DOCUMENTI, DATI E ATTREZZATURE

1. Utilizzo strumentazione

a) La strumentazione messa a disposizione degli utenti deve essere utilizzata e conservata appropriatamente; della stessa deve essere fatto un uso conforme all'obbligo di rispettare le norme di diligenza, prudenza e appropriatezza. L'Università IULM a seconda delle necessità, del ruolo e delle mansioni affidate distribuisce:

- computer fissi;
- computer portatili;
- telefoni fissi;
- telefoni portatili, sia GSM che Smartphone;
- tablet e dispostivi avanzati in grado di interconnettersi a reti telematiche e di interagire con gli altri strumenti informatici del titolare;
- dispositivi di archiviazione di massa.

b) In caso di allontanamento dalla propria postazione hardware, è fatto obbligo all'utente di attivare il salva-schermo protetto da password.

c) E' fatto obbligo di conservare, custodire e controllare i supporti informatici removibili con prudenza e valutando il pericolo che la documentazione contenuta venga utilizzata da estranei non autorizzati. Per diminuire il pericolo di accessi non autorizzati gli operatori dovranno attuare tutte le misure di sicurezza che, secondo l'ordinaria diligenza, rendono improbabile la violazione della riservatezza dei dati. Di norma, nei supporti informatici removibili vanno archiviati documenti solo in caso di effettiva necessità.

d) L'utente deve effettuare il salvataggio delle informazioni nelle cartelle di rete, in quanto sottoposte a periodici salvataggi e misure di sicurezza da parte degli amministratori del sistema informativo.

2. Accesso ed uso dei sistemi

a) L'utente si connette alla rete interna tramite la coppia di credenziali costituita da "nome utente" e "password" assegnata dagli amministratori di sistema:

- il "nome utente" identifica in modo univoco l'utente nel sistema, è pubblico e, di norma, è formato secondo la sintassi *nome.cognome*;
- la "password", inizialmente assegnata dall'amministratore di sistema, deve essere modificata dopo il primo accesso dall'utente medesimo.

b) La password è nota unicamente all'utente, è riservata e non deve essere comunicata a nessuno.

c) L'utente ha l'obbligo di cambiare la password ogni 3 mesi. Essa deve essere costituita da una combinazione alfanumerica di almeno 8 caratteri.

d) In casi eccezionali di particolare gravità e/o urgenza, per garantire la continuità operativa, gli amministratori di sistema potranno consentire, dietro espressa richiesta di un responsabile del trattamento, l'accesso alle utenze di un incaricato temporaneamente assente o impedito ad accedere autonomamente. In questo caso si procederà alla cancellazione della password e all'inserimento di una nuova. Il cambiamento della password ad opera degli amministratori di sistema è garanzia, per l'utente, che è stato effettuato da terzi un accesso autorizzato.

3. Controlli e navigazione nella rete

a) Gli incaricati possono utilizzare i computer connessi ad Internet anche per la navigazione in rete, ove la funzione lo preveda e sotto la propria responsabilità. La navigazione deve comunque avvenire nel rispetto della legge, dell'ordine pubblico, del buon costume e delle norme di prudenza e cautela atte ad evitare problemi di sicurezza al sistema informativo dell'Ateneo.

b) Per motivi di sicurezza è attivato un firewall che, a discrezione della Direzione, impedisce le attività e/o l'accesso ai contenuti classificati come pericolosi o non consentiti. Qualora si renda comunque indispensabile compiere tali operazioni è necessario rivolgere motivata richiesta in tal senso agli amministratori di sistema.

c) Qualora si ravvisino situazioni che potrebbero violare i protocolli di sicurezza, il Rappresentante del titolare, dopo aver avvisato tutti gli utenti e gli incaricati, può chiedere che vengano attivati dei controlli volti a risolvere il problema e identificarne la causa. Tale attività può coincidere anche con il controllo della navigazione su Internet effettuata in Ateneo.

d) Salvo eccezioni gli utenti non hanno la facoltà di amministrare autonomamente i computer che sono stati loro affidati. Eventuali motivate richieste di disporre dell'autorizzazione all'amministrazione del proprio computer vanno inoltrate agli amministratori di sistema, che ne valuteranno la fattibilità anche in relazione ai rischi per la sicurezza della rete di Ateneo.

4. Utilizzo posta elettronica

a. Le caselle di posta elettronica, concesse in uso al dipendente, sono destinate ad un utilizzo pertinente l'attività lavorativa.

b. In caso di impedimento da parte dell'utente di accedere alla sua casella di posta, gli Organi Direttivi dell'Ateneo possono incaricare un proprio delegato perché effettui tale accesso al fine di non interrompere, né rallentare l'attività di servizio dell'Università.

c. In caso di cessazione dal servizio del dipendente a qualsiasi titolo, l'Ufficio Risorse Umane chiede che venga configurato sul suo account di posta elettronica il "risponditore automatico". Il messaggio di risposta automatico informerà della cessazione dal servizio del dipendente stesso e fornirà un indirizzo di posta elettronica alternativo al quale rivolgersi.

   Trascorsi due mesi dalla cessazione del dipendente, l'Ufficio Risorse Umane dispone che l'account di posta elettronica venga disattivato, in modo tale da non poter più ricevere posta in arrivo.

   Le email precedentemente archiviate nell'account del dipendente cessato potranno, tuttavia, essere consultate da un delegato degli Organi di Governo dell'Ateneo, qualora ciò si rivelasse necessario ai fini dell'espletamento delle funzioni e dei servizi dell'Università.

d. E' fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica. In merito a tali informazioni, infatti, gli utenti sono tenuti al "segreto professionale" in ottemperanza agli obblighi di correttezza nei confronti del datore di lavoro.

5. Custodia, conservazione e controllo documenti cartacei

a) E' fatto obbligo all'utente di custodire il materiale cartaceo contenente dati personali con la massima cura e attenzione, affinché persone non autorizzate non ne prendano visione, né possano manipolarlo o riprodurlo.

b) Per l'archiviazione dei documenti contenenti dati personali devono essere scelti armadi, cassetti e classificatori provvisti di serrature o conservati in stanze ad accesso riservato.

c) È compito dei responsabili coordinare l'utilizzo delle chiavi in modo da assicurare l'accesso alla documentazione verificando che solo le persone che ne hanno realmente la necessità siano in grado di accedere ai documenti.

d) E' fatto divieto di lasciare documenti incustoditi in luoghi fisici o logici ad accesso indeterminato, quali stampanti di rete, fotocopiatrici, fax, cartelle di rete condivise.

6. Segreto professionale

a) L'operatore non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, *in toto* o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto dall'Università IULM, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi. Nella valutazione delle informazioni vige l'impegno a prendere ogni misura affinché le stesse rimangano segrete, essendo inteso che, in caso di divulgazione non autorizzata dagli Organi Direttivi dell'Ateneo, l'operatore dovrà fornire a questi ultimi tutte la indicazioni utili a provare di aver adottato ogni misura atta ad evitare che ciò avvenisse.

b) Gli obblighi del lavoratore, previsti in questo punto, non termineranno all'atto di cessazione del rapporto di lavoro, se non in riferimento a quelle specifiche parti delle informazioni che egli possa dimostrare essere già di pubblico dominio al momento della conclusione del rapporto o che lo siano diventate in seguito per fatto a lui non imputabile.

7. Riservatezza dati

a) Per "Informazioni riservate" si intendono tutte quelle informazioni, di qualsiasi natura, non sottoposte ad un regime di pubblicità e pubblicazione indeterminato, necessarie allo svolgimento dell'attività lavorativa e che gli incaricati conoscono per ragioni di servizio.

b) Il lavoratore si impegna ad utilizzare le informazioni riservate unicamente per svolgere l'attività cui è preposto e di conseguenza a non usare tali informazioni in modo tale da arrecare danno all'Università IULM, né per alcun altro scopo di qualsiasi natura.

c) Il lavoratore si impegna a non cancellare o distruggere alcuna informazione registrata sul proprio computer o altro strumento posseduto, custodito o controllato, qualora cessi il rapporto esistente con l'Università IULM.

d) Gli impegni di cui al presente capo non proibiscono di comunicare informazioni riservate a:

- amministratori e utenti, avvocati, revisori, banche o altri nostri consulenti ai quali la conoscenza di tali Informazioni è necessaria al fine dell'espletamento di attività funzionali all'Università IULM;
- soggetti diversi da quelli specificati al precedente punto, qualora ciò sia stato autorizzato dagli Organi Direttivi dell'Ateneo.

e) L'obbligo di riservatezza non opera in caso di Informazioni riservate che:

- al momento in cui vengono rese note siano di pubblico dominio;
- diventino di pubblico dominio dopo essere state rese note per causa non imputabile al lavoratore.

f) L'impegno di riservatezza di cui al presente capo si protrarrà anche dopo la cessazione del rapporto di lavoro e sino a quando le informazioni in oggetto non saranno rese di pubblico dominio.

8. Applicazione ed interpretazione del presente regolamento

Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, l'utente può rivolgersi al Gruppo Privacy secondo quanto indicato nell'Allegato E.