UNIVERSITÀ
DEGLI STUDI DI TRIESTE

REGOLAMENTO PER I SERVIZI WEB DI ATENEO

CONSIGLIO DEGLI STUDENTI	
SENATO ACCADEMICO	
CONSIGLIO AMMINISTRAZIONE	24.02.2017
DECRETO RETTORALE	140/2017 dd. 3/03/2017
UFFICIO COMPETENTE	*Settore Sistemi Informativi*

Data ultimo aggiornamento: *18 marzo 2017* *a cura dell'Ufficio Affari generali*

Art. 1 - Definizioni

1. Ai fini del presente Regolamento si intende:

   a) SERVIZIO WEB: Qualsiasi programma applicativo accessibile tramite una interfaccia web. Appartengono a questa categoria, in particolare, i servizi che espongono pagine informative ("siti web").
   b) AD (Active Directory): Servizio centralizzato di autenticazione ed autorizzazione utilizzato nell'Ateneo.
   c) LDAP: Protocollo per l'accesso a servizi centralizzati che mantengono informazioni organizzate in modo gerarchico, utilizzato anche per funzionalità di autenticazione ed autorizzazione.
   d) HASHED AND SALTED: Tecnica di memorizzazione delle credenziali di autenticazione sui server finalizzata a rendere più complesso l'uso delle credenziali in caso di accessi fraudolenti al server stesso. La tecnica può essere utilizzata anche in una modalità semplificata chiamata semplicemente "hashed".

Art. 2 - Ambito e finalità di applicazione

1. Il presente regolamento si applica ai servizi web ospitati sui server di Ateneo ed ha lo scopo di definire un insieme minimo di requisiti per uniformare le procedure di sviluppo e di acquisto. I requisiti sono necessari per agevolare le operazioni di manutenzione funzionale e di sicurezza dei servizi web.
2. Ai servizi web già esistenti al momento dell'entrata in vigore di queste norme si applicano gli articoli 3, 4 e 11.
3. Ai servizi web creati successivamente all'entrata in vigore di queste norme:
   a) si applicano gli articoli 3, 4 e 7 comma 1 se sviluppati con strumenti software completamente predisposti e mantenuti da Area dei Servizi ICT;
   b) si applicano gli articoli 3-10 se sviluppati con strumenti software non completamente predisposti e mantenuti da Area dei Servizi ICT.

Art. 3 - Contatti

1. Per ogni servizio web deve essere preventivamente fornita all'Area dei Servizi ICT:
   a) Nome del responsabile dei contenuti;
   b) Recapito di contatto (indirizzo struttura, telefono ed e-mail);
   c) Se il servizio tratta dati personali, nome del responsabile del trattamento. Qualora la gestione del servizio sia esternalizzata, deve essere preventivamente effettuata la nomina del legale rappresentante della società che gestisce il servizio quale responsabile del trattamento dati, a cura dell'Ufficio Protocollo e Archivio.
2. L'indirizzo email del recapito di contatto deve essere ben visibile sul servizio web, con una posizione ed aspetto grafico uniforme in tutte le componenti del servizio stesso.

Art. 4 - Presenza di contenuti inappropriati

1. Qualora l'Area dei Servizi ICT rilevi la presenza sul servizio di materiale in violazione delle leggi e regolamenti in vigore o indicativo di una intrusione, l'Area dei Servizi ICT renderà il servizio immediatamente inaccessibile. Il ripristino avverrà previa autorizzazione del Dirigente Area dei Servizi ICT e dovrà basarsi su contenuti di backup che non violino leggi e regolamenti in vigore e per i quali ci sia la ragionevole certezza dell'assenza di contenuti indicativi di intrusione (nonché su versioni software aggiornate, come specificato più sotto). L'immagine del servizio rimossa a causa della intrusione dovrà essere conservata per eventuali analisi successive.

Art. 5 - Strumenti di sviluppo

1. Prima di iniziare lo sviluppo e l'eventuale formalizzazione del contratto con un fornitore esterno, è necessario concordare con Area dei Servizi ICT l'effettiva possibilità di utilizzare gli strumenti software proposti. La proposta deve essere accettata dal Dirigente Area dei Servizi ICT, sentito il Delegato del Rettore ai Sistemi Informativi.

Art. 6 - Responsabile della manutenzione

1. Prima della entrata in produzione dovrà essere specificata l'identità dell'amministratore o dell'azienda responsabile per la manutenzione del servizio e la data di eventuale scadenza del contratto. Queste informazioni, così come le informazioni di cui all'articolo 3, dovranno essere confermate o rinnovate con scadenza annuale.

Art. 7 - Entrata in produzione del servizio

1. Prima dell'entrata in produzione è necessario il collaudo effettuato con il personale tecnico dell'Area dei servizi ICT, atto a verificare la rispondenza dei requisiti indicati nel presente Regolamento. La mancata rispondenza di uno solo dei requisiti richiesti preclude la messa in produzione del sito.
2. Prima della entrata in produzione dovrà essere specificato l'insieme di strumenti software utilizzati con i rispettivi numeri di versione, in particolare, il sistema di gestione dei contenuti, il sistema di gestione del database, le principali librerie.
3. Alla data di entrata in produzione il fornitore dovrà certificare quanto segue, fornendo ad Area dei Servizi ICT tutte le informazioni utili per verificare quanto certificato:
   a) Livello di aggiornamento degli strumenti software utilizzati;
   b) Tutte le utenze di default siano state disabilitate, tutte le password di default siano state modificate, tutte le porte non strettamente necessarie per il funzionamento siano state

chiuse. L'utenza di amministrazione del servizio può rimanere abilitata ma con password non di default.

Art. 8 - Manutenzione

1. La manutenzione effettuata durante la produzione deve comprendere, per tutti gli strumenti software utilizzati, il rapido aggiornamento di tutte le vulnerabilità di livello critico rese note pubblicamente nei principali forum specializzati. Il reperimento di queste informazioni deve essere a cura del responsabile della manutenzione. Area dei Servizi ICT e il Delegato del Rettore ai Sistemi Informativi possono chiedere il rapido aggiornamento anche di vulnerabilità di livello non critico, sulla base di esigenze specifiche dell'ambiente locale.

Art. 9 - Protocolli di accesso e di autenticazione

1. L'intero servizio web deve essere reso accessibile solo via HTTPS. In particolare, la configurazione preferibile è quella in cui il servizio non fornisce nessun contenuto via HTTP. Configurazioni in cui contenuti richiesti via HTTP sono serviti con una reindirizzamento alla home page del servizio su HTTPS sono accettabili.
2. Se il servizio prevede una sezione con accesso autenticato:
   a) Le utenze già inserite nel sistema AD di Ateneo devono essere preferibilmente autenticate con uno dei sistemi di autenticazione federata supportati in Ateneo o, in alternativa, con interrogazione LDAP su canale sicuro al sistema AD di Ateneo. Il servizio non deve memorizzare localmente le credenziali di autenticazione per queste utenze.
   b) Le utenze non inserite nel sistema AD di Ateneo possono essere autenticate localmente dal servizio. Le credenziali di autenticazione devono essere memorizzate in modalità hashed e salted, oppure in modalità hashed nel solo caso in cui siano usate tecnologie basate su Microsoft Windows.

Art. 10 - Mancato rispetto delle norme

1. Il mancato rispetto di una di queste norme in produzione può comportare l'immediato spegnimento del servizio fino al dimostrato ripristino. Ad esempio, un servizio con contratto di manutenzione scaduto può essere reso inaccessibile senza preavviso, fino al ripristino della manutenzione e delle versioni software più aggiornate. Per lo spegnimento del servizio potranno essere adottate misure arbitrarie di isolamento. In casi eccezionali e di particolare gravità, queste misure possono comportare l'isolamento di altri servizi che non sono in violazione di queste norme.

Art. 11 - Norme transitorie

1. Per i servizi web già esistenti all'entrata in vigore di queste norme:
   a) Il responsabile dei contenuti dovrà specificare l'insieme di strumenti software utilizzati con i rispettivi numeri di versione, in particolare, il sistema di gestione dei contenuti, il sistema di gestione del database, le principali librerie.
   b) Il responsabile dei contenuti dovrà specificare l'identità dell'amministratore o dell'azienda responsabile per la manutenzione del servizio e la data di eventuale scadenza del contratto.
   c) Area dei Servizi ICT e il Delegato del Rettore ai Sistemi Informativi concorderanno con i responsabili della manutenzione tempi e modalità per:
      1) rilevare il grado di aderenza del servizio alle norme sopra descritte;
      2) predisporre ed eseguire azioni correttive.

2. Qualora le azioni correttive non possano essere effettuate o non possano essere completate in tempi rapidi, è facoltà del Dirigente Area dei Servizi ICT, sentito il Delegato del Rettore ai Sistemi Informativi, procedere allo spegnimento del servizio. Ciò dovrà essere effettuato solo in casi eccezionali ed in presenza di vulnerabilità o di rischi particolarmente gravi (a titolo esemplificativo ma non esaustivo: invio di credenziali di autenticazione su canale non crittato, vulnerabilità altamente critica su uno strumento software molto diffuso, servizio senza manutenzione sistemistica da tempo). Il servizio potrà essere reso nuovamente accessibile solo previo parere favorevole del Dirigente Area dei Servizi ICT, sentito il Delegato del Rettore ai Sistemi Informativi.
3. Qualora non sia possibile ottenere le informazioni specificate al comma 1, è facoltà del Dirigente Area dei Servizi ICT, sentito il Delegato del Rettore ai Sistemi Informativi, procedere allo spegnimento del servizio come indicato nell'articolo 10.