Uso delle risorse di rete dell'Università di Trieste

Status: in vigore

Versione documento: 1.3.3

Ultima modifica: 2025/08/20 15:20 (%f)

Scopo del documento

Il documento descrive alcuni servizi di rete e le relative regole d'uso per l'utente dell'Università di Trieste e rappresenta le norme tecniche emanate dal Gestore come previsto dal Regolamento di Accesso al Sistema Integrato di Reti dell'Ateneo (SIRA), da qui in poi abbreviato “regolamento SIRA”.

In particolare l'assegnazione delle credenziali di accesso ad elaboratori, reti e servizi gestiti dall'Area dei servizi ICT è subordinata all'accettazione delle regole di comportamento descritte in:

- questo documento
- regolamento di Accesso al Sistema Integrato di Reti dell'Ateneo (SIRA)
- GARR AUP in Italiano e in Inglese
- Netiquette Guidelines rfc1855 (inglese)
- Guidelines for Mass Unsolicited Mailings (spam) rfc2635 (inglese)

che sono a tutti gli effetti parte di questo documento.

Reperimento informazioni sulle regole

Questo documento è disponibile sui server dell'Università all'URL **https://www.units.it/normeusorete**. Gli utenti sono invitati a leggere almeno una volta questo documento (perlomeno le parti di loro particolare pertinenza) e di impegnarsi ad osservare le regole che l'Università a sua volta deve rispettare con i partner negli accordi nazionali ed internazionali.

Poiché il mondo informatico evolve rapidamente le regole possono cambiare abbastanza frequentemente. Per tale motivo l'utente è invitato a consultare periodicamente il documento di storicizzazione delle regole almeno una volta ogni due mesi.

Note sui servizi

Su ciascuna risorsa può essere imposto un limite d’uso (es. di tempo di CPU, di spazio disco, di banda, ecc.) che ciascun utente è tenuto a rispettare per un buono sfruttamento dei servizi da parte di tutti.

Linee guida per la gestione di servizi di rete

Il collegamento sulla rete di Ateneo di apparecchiature atte a erogare servizi in rete quali ad esempio server web, postali, access point wireless, server dhcp, ecc. è regolato dalle Linee guida per la gestione di servizi di rete

Posta elettronica

Agli utenti che abbiano ottenuto l'accesso a servizi informatici dell'Università viene riconosciuto il diritto di disporre di almeno una casella postale personale.

Ogni struttura che fornisca un servizio postale autonomo, lo eroga come ritiene più opportuno per i suoi utenti in armonia con i vincoli tecnici disposti dal Regolamento di Ateneo SIRA e quanto formulato dal Nucleo di Sicurezza Informatica (NSI).

L'uso della posta elettronica è sottoposto ad alcuni vincoli che l'utente universitario è tenuto ad osservare:

Contenuti sensibili

I dati sensibili così come individuati dalle leggi italiane vigenti, o in generale riservati, vanno crittografati prima di essere inviati.

Dimensione

La posta elettronica dovrebbe essere impiegata solo per l'invio di testi di non più di qualche pagina di testo, soprattutto se sono coinvolti nodi esterni al comprensorio universitario.

File (anche di testo) di grandi dimensioni vanno trasferiti in modo diverso (per es. con servizi di trasferimento file di grosse dimensioni come Filesender).

```
  Si deve tener conto che i mail vengono gestiti da server postali che
trasferiscono
  interi messaggi postali da un nodo all'altro.
  Questo implica che se c'è una coda di messaggi da smaltire (e a livello
universitario
  le code possono raggiungere consistenze di migliaia di mail)
  ogni mail di grandi dimensioni blocca l'intera coda finché non viene
smaltito
  (cioè comunicato al prossimo nodo postale).
  Inoltre i nodi postali intermedi tra il nodo origine e quello destinazione
devono
  memorizzare i mail in transito e se questi mail sono di grandi dimensioni,
  l'impegno richiesto dai nodi intermedi è ingiustificatamente oneroso.
```

Liste di posta elettronica

La pratica di iscriversi a delle liste di posta elettronica, va seguita con cautela seguendo alcune precauzioni:

- quando ci si iscrive ad una lista si ricevono uno o più mail di risposta che confermano l'iscrizione e contengono le istruzioni di cancellazione ed il comportamento richiesto per quella lista. L'utente è pregato di leggere questi mail. È anche pregato di conservare questi mail di accettazione perché saranno utili quando ci si vorrà disiscrivere (cosa che potrebbe risultare necessaria non solo nel caso di disinteresse per la lista, ma anche, per es. quando si voglia far recapitare i messaggi su account o elaboratore diverso oppure quando cessa il rapporto con l'Università e si liberano le risorse impiegate);
- chi si iscrive ad almeno una lista non può più impiegare risponditori postali automatici perché così risponderebbe automaticamente alle liste (anche se i gestori di lista spesso sono abbastanza intelligenti da filtrare risposte involontarie).
- attenzione all'indisponibilità del destinatario postale iscritto alla lista (cioè il proprio account). Se per caso il destinatario non può ricevere posta (per es. perché ha superato la quota disco, o perché ha un forward o inoltro automatico verso un elaboratore indisponibile) il mail torna indietro al gestore postale della lista e talvolta la lamentela non arriva al destinatario postale (appunto irraggiungibile), ma al gestore dell'elaboratore presso il quale l'utente ha l'account iscritto alla lista;
- quando termina il rapporto con l'Università si è pregati di cancellarsi da tutte le liste;
- dal momento in cui si richiede la cancellazione a quello in cui questa avviene, può passare diverso tempo.

Uso consentito dell'indirizzo email

I dipendenti universitari possono indicare il proprio indirizzo email universitario nel proprio biglietto da visita e nella carta intestata, purché ambedue siano relativi all'Università o ad altro Ente con essa convenzionato.

Controlli automatici e garanzie

La posta elettronica viene sottoposta a controlli automatici.

I messaggi di posta elettronica che risultano positivi ai test antivirus possono venire soppressi senza alcuna comunicazione al mittente e al destinatario per tutelare la sicurezza e il buon funzionamento del servizio, dei personal computer, della rete e di sistemi, servizi e reti non universitari.

I messaggi non richiesti che mirano al furto delle credenziali (phishing) o commerciali di massa (spam vero e proprio) vengono marcati come “spam” e cancellati automaticamente, tuttavia il procedimento di riconoscimento ha un margine di errore intrinseco per cui alcuni messaggi, marcati e non, vengono comunque recapitati all'utente. È vivamente consigliato all'utente di cancellarli utilizzando l'opportuna funzionalità di “segnala come phishing” o “segnala come spam” per migliorare i sistemi automatici a beneficio di tutti.

La consegna dei messaggi a destinazione non è garantita. Solitamente problemi bloccanti nel recapito vengono segnalati al mittente, tuttavia anche questo non è garantito. Per avere la certezza della

consegna al destinatario si consiglia di utilizzare il meccanismo delle ricevute di lettura dei messaggi implementate nei client di posta elettronica.

I tempi di consegna dei messaggi di posta elettronica sono variabili, solitamente sono di pochi secondi ma in alcuni casi possono passare ore o anche giorni. La posta elettronica NON è un sistema di messaggistica istantanea.

Collegamento di dispositivi alla rete di Ateneo

Riferimento *Articolo 7 Regolamento SIRA*

Per collegare un personal computer, un notebook, un server, una stampante, ecc. alla rete di Ateneo in modo che divenga un nodo della stessa, bisogna procedere alla sua registrazione presso l'Area dei Servizi ICT a meno che la rete a cui ci si collega non sia dotata di accesso autenticato e configurazione automatica dell'indirizzo.

Di ogni nodo connesso in rete dev'essere data comunicazione all'Ufficio Reti e telefonia dell'Area dei Servizi ICT e ai Referenti di Rete delle singole strutture che conoscono la struttura, le connessioni e filtrano i problemi.

Evitare in ogni modo di inserire o spostare un elaboratore dalla rete senza aver contattato un Referente di Rete locale o dell'Area dei Servizi ICT: indirizzi errati (per es. preimpostati in fabbrica o validi in altra rete) potrebbero causare danni anche rilevanti al funzionamento della rete.

Normalmente, per ragioni di protezione da attacchi informatici, gli indirizzi IP assegnati non sono contattabili da internet; se il nodo deve fungere da server o adottare protocolli particolari, ciò va segnalato e viene conseguentemente assegnato un indirizzo pubblico con solo le opportune aperture dall'esterno. Tutti i nodi connessi alla rete di ateneo hanno l'obbligo di essere costantemente aggiornati, sia come software antivirus, sia per quanto riguarda gli aggiornamenti di sicurezza del Sistema Operativo.

Il responsabile di ogni nodo in rete dev'essere a conoscenza delle leggi vigenti in materia e risponde in prima persona delle attività svolte in rete da quel nodo, in prima istanza anche in caso di compromissione da parte di cracker.

Dispositivi IoT

Data la dimostrata insicurezza e lentezza da parte dei produttori al rilascio di aggiornamenti efficaci, i dispositivi di categoria Internet of Things vanno configurati con indirizzi IP privati, non ruotati all'esterno dell'università di Trieste e possibilmente ulteriormente isolati dal traffico client e server. L'accesso dall'esterno dell'Università di Trieste avviene tramite l'utilizzo di VPN. L'accesso in uscita ad Internet può essere attivato se necessario tramite proxy o NAT.

La tipologia IoT comprende, a titolo di esempio non esaustivo, stampanti, dispositivi di illuminotecnica, videoproiettori, schede di controllo di apparati di refrigerazione e riscaldamento, macchine di laboratorio, telecontrollo di centrali, telecamere di videosorveglianza, remotizzatori di attuatori elettrici o idraulici, attuatori pirotecnici, ecc…

Sono escluse dalla necessità di indirizzamento privato eventuali webcam di tipo enterprise

posizionate in modo da non riprendere persone, targhe o altri soggetti tutelati dalla normativa sulla privacy.

Credenziali di accesso

Forma

Le credenziali di accesso possono essere costituite, a seconda dei servizi a cui si ha accesso, dalla coppia username/password, token di autenticazione (chiave usb o smartcard), certificati.

Rilascio

Le credenziali vengono rilasciate a persone fisiche dagli uffici preposti a seconda della tipologia di utenza (Segreterie studenti, servizio accrediti dell'Area dei Servizi ICT, uffici decentrati, ecc...) previo riconoscimento della persona anche tramite richiesta di documento di identità valido a norma di legge.

Custodia

Le credenziali di autenticazione sono strettamente personali e non cedibili ad alcuno nella conoscenza o nell'uso. La cessione abusiva o l'incauta custodia possono comportare al titolare delle credenziali conseguenze di tipo civile o penale per le azioni perpetrate, sia da accesso locale sia da accesso remoto, con tali credenziali. È possibile cambiare in qualsiasi momento autonomamente, via web, la password di accesso. Si consiglia a tal proposito di cambiare frequentemente la password di accesso scegliendola di almeno 8 caratteri alfanumerici in modo che non abbia senso compiuto in alcuna lingua. A tal proposito l'Area dei Servizi ICT può mettere in atto sistemi automatici che impediscano l'immissione di password troppo semplici o già usate in precedenza. Gli account con password immutata per un periodo superiore ai 5 anni possono venire bloccati.

Durata

Le risorse informatiche universitarie (in particolare le credenziali di accesso) possono essere impiegate fino a che sussiste un rapporto lavorativo o di iscrizione con l'Università (dipendenti o iscrizione regolare a corsi di laurea o di diploma o di specializzazione, a master, ecc.).

Allo scadere del rapporto la risorsa va liberata nel minor tempo possibile.

I dati presenti sui sistemi accessibili con le credenziali assegnate possono venire irrimediabilmente distrutti dopo 6 mesi dal blocco dell'accesso al servizio.

D'altra parte, prima della scadenza naturale data dalla cessazione del rapporto, le risorse non verranno revocate a meno di richiesta esplicita o per gravi motivi.

Registro degli accessi e delle attività svolte

Gli accessi alle risorse informatiche e di rete vengono registrati. I dati così raccolti vengono usati per:

- Erogazione del servizio
- Analisi di malfunzionamenti
- Statistiche sull'utilizzo delle risorse previa anonimizzazione dei dati
- Gestione di eventuali incidenti di sicurezza

I dati identificativi della persona insieme ai registri degli accessi vengono consegnati unicamente su richiesta all'autorità competente nell'ambito di indagini giudiziarie come previsto dalla normativa vigente.

Il contenuto delle comunicazioni non viene registrato sebbene alcune voci del registro possano essere indicative della tipologia dei contenuti.

Memorizzazione di dati sensibili

I dati sensibili così come individuati dalla normativa italiana vigente, non vanno salvati su file server o altro tipo di elaboratori, compreso il pc personale o dispositivi palmari collegati in rete e che non siano espressamente adibiti allo scopo.

Eventuali elaboratori su cui vengano conservati dati personali e/o sensibili e sui quali devono essere messe in pratica tutte le misure minime ed idonee previste dalla normativa 196/2003, devono essere segnalati dal Capo Struttura all'Amministrazione Centrale attraverso le apposite procedure.

Sanzioni

La non osservanza delle regole ed un uso scorretto del servizio potrà dar luogo ad una progressiva disabilitazione dei servizi e, nei casi previsti, a sanzioni disciplinari.

Normativa di riferimento

- Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica legge n. 547 del 23 dicembre 1993
- T.U. sulla Privacy D.L. 30 giugno 2003 n. 196
- Amministratore di Sistema Provvedimento Garante privacy 27/11/2008, G.U. n. 300 del 24 dicembre 2008.
- Legge “Pisanu” - misure Antiterrorismo - D.M. 16 Agosto 2005 n. 19023 - pubblicato nella Gazz. Uff. 17 agosto 2005, n. 190
- Codice di comportamento dell'Università degli Studi di Trieste, Art. 11 - Comportamento in servizio, comma 7: *“Il lavoratore custodisce con particolare cura e diligenza gli strumenti informatici, nonché le credenziali di accesso ai sistemi informativi messi a disposizione dall’Ateneo, anche al fine di non pregiudicarne la sicurezza informatica.”*
- Codice di comportamento dell'Università degli Studi di Trieste, Art. 12 - Rapporti con il pubblico,

comma 5: *“Il lavoratore deve essere chiaro ed esaustivo nel fornire le risposte alle varie istanze ricevute; se l’istanza è formulata in via telematica il lavoratore si impegna ad utilizzare lo stesso strumento con cui è stata inoltrata la stessa, provvedendo ad istruire la risposta con tempistiche rispondenti al tenore del quesito e comunque adeguate agli standard di efficienza. Devono inoltre essere sempre evidenziati tutti gli elementi idonei ai fini dell’identificazione del responsabile della risposta. Le risposte, qualora non determinino l’attivazione di procedimenti amministrativi, sono inoltrate di norma entro 15 giorni e, comunque, non oltre 30 giorni, salvo giustificato motivo.”*

- Regolamento in materia di utilizzo della posta elettronica e della rete internet messi a disposizione dall'Università di Trieste