Università di Foggia

REGOLAMENTO PER LA CYBERSICUREZZA DI ATENEO

Area Sistemi Informativi

V.4 del 23/09/2025

Sommario

Regolamento per la cybersicurezza della rete di Ateneo

I server fisici o virtuali che erogano in rete un servizio informatico in nome e per conto dell'ateneo, cioè tutti server centrali gestiti dalle divisioni tecniche dell'università e ogni altro server che debba fornire un servizio ufficiale di ateneo, devono uniformarsi alle particolari direttive di sicurezza e continuità del servizio descritte di seguito.
In particolare le direttive per questi server riguardano:

- Sicurezza fisica/controllo accessi
- Continuità del servizio/disaster recovery
- Integrità dati e sistemi
- Antivirus/worm/trojan
- Aggiornamenti dei sistemi operativi
- Gestione delle password
- Management locale e remoto
- Logs di sistema e loro controllo
- Configurazioni di base per la sicurezza
- Interventi sui sistemi da parte di personale esterno

I servizi ufficiali erogati dall'ateneo devono uniformarsi al regolamento descritto nel seguito. In particolare le direttive per questa tipologia di servizi riguardano:

- Privilegi dei servizi
- Aggiornamenti
- Gestione delle password
- Accessi ai servizi
- Logs e loro controllo
- Statistiche sui servizi offerti

Soggetti Coinvolti

Il presente documento è rivolto alle strutture centrali e/o dipartimentali che decidono di implementare servizi informativi o servizi di rete.
Ogni utente è tenuto ad adottare, nell'ambito delle proprie attività, tutte le misure di sicurezza atte a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle risorse informatiche; devono pertanto essere prontamente segnalati furti, danneggiamenti o smarrimenti di tali strumenti.
Ciascun utente che operi nell'ambito dell'Ateneo è tenuto ad uniformarsi alle sopraddette prescrizioni.
È vietata qualsiasi attività che possa produrre danni alle risorse informatiche dell'Ateneo o che risulti in contrasto con le regole contenute nel presente regolamento o con le nome vigenti in materia.

Art. 1) La rete di ateneo.

La rete di ateneo è costituita:

- dalla rete di collegamento telematico tra tutte le varie sedi di UNIFG (WAN o rete di Backbone);
- dalle sottoreti (LAN) afferenti ai vari dipartimenti di cui è composta UNIFG;
- dai servizi di gestione della rete;
- dai servizi applicativi di base forniti sulla rete, quali Proxy, VoIP, Web;
- dal servizio di accesso remoto via tunnel VPN;
- da tutti quegli strumenti di interoperabilità e apparati attivi di rete che permettono ai soggetti autorizzati di accedere alla rete e di comunicare tra loro.

Art. 2) Protocolli consentiti.

Nella rete di ateneo viene garantito il supporto per la suite di protocolli TCP/IP, le strutture possono utilizzare al loro interno anche altri protocolli, dandone comunicazione preventiva al servizio reti, a patto che essi rimangano totalmente confinati all'interno delle strutture medesime. La propagazione di altri protocolli di rete (per esempio Decnet, Appletalk, NetBeui, ecc.) non può essere consentita esternamente alle strutture. In casi particolari (per esempio se la Struttura è distribuita su più edifici), di concerto tra il servizio reti e la Struttura, verrà studiata la fattibilità tecnica dell'utilizzo di un altro protocollo che graviti su parte della rete di Ateneo. In caso positivo verrà adottata una soluzione che comunque non influisca sull'affidabilità e sulle prestazioni della rete.

Art. 3) Elenco dei soggetti che possono accedere alla rete.

La rete viene fornita alle strutture dell'ateneo e agli Enti e Organizzazioni universitarie esplicitamente autorizzate dal CdA dell'ateneo.

L'accesso alla rete è consentito solo a studenti, docenti e ricercatori dell'ateneo, personale tecnico-amministrativo dell'ateneo, borsisti, dottorandi, assegnisti, cultori della materia afferenti all'ateneo e ad altri soggetti esplicitamente autorizzati dal responsabile della struttura di riferimento.

Per quanto riguarda gli studenti, l'accesso avviene dai laboratori informatici, dalle aule informatiche, dalle biblioteche, dalle postazioni fisse nelle stanze associative e dai propri dispositivi personali.

Art. 4) Accesso alla rete dalle postazioni per il pubblico presenti nelle biblioteche.

Le biblioteche possono fornire i servizi bibliotecari disponibili in rete di ateneo a tutti i propri utenti, attraverso postazioni presenti al loro interno e collegate alla rete di ateneo. Tali postazioni sono soggette ai criteri di sicurezza previsti per gli host in rete e in aggiunta devono soddisfare le seguenti regole:

- Gli utenti non devono mai accedere al sistema con i privilegi di amministratore, non deve essere possibile l'installazione di applicativi di qualsiasi genere;
- Gli applicativi utilizzabili dall'utente devono essere soltanto quelli consentiti;

- L’utente deve essere preventivamente informato, qualora si utilizzi un sistema di monitoraggio/filtraggio dei dati in transito applicato al fine di verificare il corretto utilizzo della postazione.

L’utilizzatore deve necessariamente essere identificato e tale identificazione può avvenire mediante un sistema di autenticazione automatico sicuro, in grado di identificare ed autorizzare sulla base di credenziali fornite dall’utente. Le credenziali minime sono la coppia username e password, personali e non cedibili.
Tale sistema di autenticazione e autorizzazione può anche essere locale, cioè appoggiarsi a una base dati locale di competenza e responsabilità della singola biblioteca o di più biblioteche.
Nel caso non si potesse disporre di un sistema di autenticazione e autorizzazione automatico, bisogna individuare un referente all’interno della struttura che identifichi, a mezzo di registri, il soggetto che utilizza la postazione (segnando il momento di accesso alla macchina – login - e il momento di uscita - logout). Tali attività esauriscono i compiti di presidio dei soggetti preposti alla cura delle postazioni pubbliche e del loro utilizzo. Ogni necessario intervento del personale preposto al presidio, nel caso ci sia il sospetto di un utilizzo non idoneo del mezzo telematico, è ammesso nel rispetto della privacy dell’utilizzatore della postazione.

Art. 5) Accesso alla rete via linee commutate.

Il servizio di accesso remoto messo a disposizione dal servizio reti di Ateneo è disponibile per alcune tipologie di utenti della rete: docenti, ricercatori, borsisti, dottorandi, dipendenti dell’ateneo. Username e password sono strettamente personali e non cedibili a terzi. L’utilizzo di router o access point personali è vietato, a meno di casi particolari relativi a specifiche esigenze, che devono essere concordati con il servizio reti. Qualora una struttura intenda intraprendere soluzioni autonome per la fornitura di accesso remoto, deve darne preventiva comunicazione al servizio reti e al servizio sicurezza di rete, garantendo l'adozione di tutte le misure di sicurezza atte a prevenire intrusioni e/o utilizzi illeciti attraverso linea commutata. L'attività può essere intrapresa solo a seguito del riconoscimento da parte del servizio reti e del servizio sicurezza di rete dell'idoneità delle misure di sicurezza adottate.

Art. 6) Accesso/estensioni della rete, via VPN o sistemi di tunnelling.

Estensioni della rete di Ateneo, temporanee o permanenti, via VPN o altri meccanismi di tunnelling analoghi sono vietate, a meno di casi particolari da concordarsi con il servizio reti e sotto la supervisione del gruppo sicurezza di rete. Sono consentiti singoli tunnel VPN verso utenti autorizzati per permetterne l’accesso da reti esterne a quella di ateneo. Il servizio è disponibile per alcune tipologie di utenti dell’ateneo: docenti, ricercatori, dipendenti, aziende esterne che riscontrino l’esigenza di operare come se fossero connessi direttamente alla rete di ateneo dalla loro sede remota (ad es. per l’utilizzo di particolari programmi applicativi, per l’accesso a dati sensibili o nel caso dei telelavoratori). Il concentratore di VPN per l’accesso dell’utenza in questa modalità viene gestito centralmente dal servizio reti; gli utenti connessi vengono mappati su una sottorete di UniFG dedicata. Qualora una struttura necessiti, per particolari esigenze, di fornire ai propri utenti accessi VPN terminati all’interno delle proprie LAN, dovrà richiederne autorizzazione preventiva al servizio reti e al gruppo sicurezza di rete. La richiesta dovrà contenere la motivazione della scelta di questo tipo di accesso e il numero di utenti previsto, per permetterne una corretta valutazione. La struttura si fa carico del server per la concentrazione

delle VPN in tutti i suoi aspetti, conformandosi alle norme di sicurezza descritte in questo documento, in particolare gli utenti devono essere autenticati.

Art. 7) Le reti wireless.

L'implementazione di una rete via radio (wireless) comporta a tutti gli effetti un'estensione della rete di ateneo, e risulta quindi soggetta a tutte le regole stabilite per le sottoreti dell'università. In particolare non è consentito implementare in proprio un tale tipo di rete senza l'intervento del servizio reti. Come le sottoreti cablate dell'università anche queste reti devono essere progettate e realizzate dal servizio reti in accordo con la struttura che ne ha fatto richiesta o per la quale questo tipo di tecnologia è stata ritenuta più idonea dal servizio reti per soddisfare particolari esigenze ambientali o di mobilità. L'utilizzo delle reti wireless deve essere giustificato da una effettiva esigenza che richieda questo tipo di soluzione, in ragione degli inconvenienti che tale scelta comporta (basse velocità, intercettabilita', estensione del campo d'azione al di fuori dei confini universitari, sicurezza). Per quanto riguarda la sicurezza, l'implementazione della soluzione wireless deve essere tale da garantire l'accesso soltanto agli utenti abilitati (autenticazione preferibilmente 802.1x) e deve prevedere la crittazione del traffico (riservatezza), per portare il livello di sicurezza di questo tipo di reti allo stesso livello garantito da quelle cablate.

Art. 8) La rete Eduroam

Il servizio WiFi Eduroam è dedicato principalmente a Studenti, Docenti, Dottorandi, Ricercatori e Tecnici-Amministrativi.
La richiesta di account può essere inoltrata anche da utenti temporanei (visiting researcher ed ospiti dell'Università a vario titolo, espressamente autorizzati attraverso una richiesta diretta da inoltrare alla segreteria del polo di riferimento o presso gli uffici dei referenti tecnici di Dipartimento.
La registrazione comporta l'accettazione integrale della AUP (Acceptable Use Policy) del GARR, del Regolamento sulle condizioni d'uso dell'Università di Foggia con l'impegno di utilizzare la rete ed i servizi offerti nel pieno rispetto della "netiquette" ed in conformità alle attuali norme vigenti.
L'utente accetta inoltre di aderire al servizio WiFi nella piena consapevolezza che i log del traffico generato verranno memorizzati e custoditi per un tempo non inferiore a sei mesi, in accordo con le attuali norme di legge.
Il trattamento dei dati avviene secondo l'informativa privacy disponibile su https://www.unifg.it/privacy. Gli interessati possono esercitare i diritti di cui agli artt. 15-22 GDPR contattando il DPO all'indirizzo dpo@unifg.it.
Condizioni e norme di utilizzo consultabili al link https://www.unifg.it/sites/default/files/2021-08/eduroam-regolamento.pdf

Art. 9) Assegnazione degli indirizzi IP e sotto-domini logici della gerarchia UniFG.it.

Gli indirizzi IP per gli host all'interno della rete di ateneo vengono assegnati dal servizio reti, in modo statico o dinamico (DHCP) . Il piano di indirizzamento IP della rete di ateneo è amministrato dal servizio reti. Il server DNS relativo a questo piano di indirizzamento è curato e mantenuto dall'Area sistemi Informativi. La gestione di server DNS primari all'interno delle sottoreti va

concordata con il servizio reti, il quale fornirà presso i suoi server centrali il servizio di DNS secondario per tali server primari locali.

Art. 10) Host multi-homed.

La presenza all'interno della rete di Ateneo di host multi-homed va autorizzata dalla struttura competente e concordata con il servizio reti, per evitare problemi di routing e di naming. Il traffico relativo alle diverse reti a cui tali host possono essere collegati va mantenuto separato.

Art. 11) Identificazione dei soggetti in rete

Tutti gli utenti a cui vengono forniti accessi alla rete di Ateneo devono essere riconosciuti ed identificabili; è vietata l'assegnazione di password collettive o non riconducibili ad un singolo soggetto fisico.

Art. 12) Inserimento in rete di un host.

Per inserire un host nella rete di ateneo è necessario:

- Richiedere un indirizzo IP al servizio reti o ai responsabili di dipartimento oppure configurare la macchina per riceverlo dinamicamente a seconda delle istruzioni ricevute dal servizio reti o dai responsabili di dipartimento.
- Installare una protezione antivirus di ateneo.
- Controllare se la macchina offre servizi di rete e in caso affermativo eliminarli tutti
- Applicare tempestivamente tutte le patches di sicurezza del sistema e degli
- applicativi di cui si intende fare uso e mantenerne nel tempo l'aggiornamento

La persona a cui la macchina in rete è data in consegna è ritenuta responsabile per quella macchina e per la sua attività nella rete di ateneo

Art. 13) Limiti di utilizzo della rete da parte degli host.

Un host che produce un grande flusso di dati in rete diviene fonte di problemi per la rete che lo ospita, in questi casi il servizio reti potrà limitare l'utilizzo della banda trasmissiva da parte di singoli hosts. Per server o host che necessitino di produrre un elevato volume di traffico è necessario il permesso preventivo del servizio reti e comunque va con esso concordata una soluzione che incida il meno possibile sulla sottorete d'appartenenza e sulla rete di ateneo.

Art. 14) Servizi erogati in rete da parte delle strutture periferiche.

Per tutti i servizi di rete che vengono erogati da host appartenenti alla rete di Ateneo è necessario individuare uno o più responsabili che si occupino in maniera continuativa dell'oggetto messo in rete. I servizi che devono essere visibili al di fuori della rete locale della struttura devono venir registrati a livello centrale dalle strutture di competenza, la registrazione comprende i dettagli dell'implementazione (tipo di servizio, nome e versione dell'applicativo che lo realizza eventuali funzioni accessorie e loro caratterizzazione) dell'accessibilità del servizio (quali utenti sono autorizzati a fruirne, meccanismo di autenticazione, stima del numero massimo possibile di utenti),dei tempi di operatività (data di start-up del servizio, eventuale data di dismissione, tempi in cui il servizio è operativo [es 24x7x365 per servizi sempre on line]) e i dati relativi ai responsabili del servizio sia amministrativi che tecnici. Gli elaboratori messi in rete per erogare uno o più servizi devono limitarsi a questi: tutti i servizi non necessari vanno spenti. I server vanno costantemente aggiornati, sia per i problemi di sicurezza del software relativo ai servizi erogati,

sia nelle patches di sicurezza del sistema operativo che li supporta. I servizi devono essere contattabili e utilizzabili soltanto da coloro i quali sono autorizzati a farlo; ovvero bisogna autenticare gli utenti, o le macchine, o le reti che devono poter accedere al servizio. Ovviamente i server pubblici sono contattabili da chiunque nel mondo. I server eseguono il logging delle connessioni e lo mantengono, ove tecnicamente possibile, per un periodo di un anno. I server vanno tenuti sincronizzati con il server di sincronizzazione di ateneo o un server NTP su GMT+1(ora legale) e MT+2(ora solare) per permettere una corretta interpretazione dei log. L'accesso privilegiato al sistema deve essere riservato al solo amministratore in modalità locale o in modalità cifrata se effettuato da remoto (ad esempio tramite il protocollo SSH) . Devono essere messe in atto almeno tutte le procedure minime per la sicurezza del sistema che ospita il servizio e sul servizio stesso, compresa la protezione contro virus informatici, laddove necessaria, e la protezione fisica della macchina da accessi incontrollati.

Art. 15) Attività di logging.

Il servizio reti opera un'attività di logging sui router e switch della rete allo scopo di produrre statistiche di utilizzo, occupazione di banda e per tipologia di servizio/protocollo atte ad ottimizzare i flussi di dati entro la rete di Ateneo.
Le strutture che offrono servizi informatici sono tenute a conservare le registrazioni degli accessi per i seguenti periodi:

- Log di autenticazione: 6 mesi per finalità di sicurezza (base giuridica: legittimo interesse art. 6.1.f GDPR);
- Log relativi a indagini in corso: fino a conclusione del procedimento;
- Decorsi i termini, i dati devono essere cancellati o anonimizzati irreversibilmente.

Le strutture devono assicurare all'utenza che dette registrazioni non siano disponibili ad alcuno se non nei casi di emergenza o di indagine, nel rispetto del Regolamento UE 2016/679 (GDPR), del D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018 e dei provvedimenti del Garante Privacy.

Art. 16) Provvedimenti verso i trasgressori.

In caso di accertata inosservanza delle norme di utilizzo della rete, l'organismo incaricato prenderà le opportune misure, necessarie al ripristino del corretto funzionamento della rete, compresa la sospensione dell'accesso alla rete stessa da parte del trasgressore per motivi cautelari. In caso di reiterata inosservanza, per colpa grave o dolo, il trasgressore sarà suscettibile di provvedimento disciplinare secondo la normativa vigente. In caso di misure d'emergenza, tese a salvaguardare il funzionamento della rete nel suo insieme o in una delle sue parti (es: attacchi D-DOS, worm ecc.), il Servizio Reti può, come misura transitoria, attuare una sospensione parziale o totale all'accesso alla rete di un singolo o di un'intera LAN, oppure di uno o più servizi di rete o effettuare una riduzione anche drastica nella banda assegnata a una certa struttura o su un particolare link WAN.
In caso di violazione dei dati personali (perdita, distruzione, modifica, divulgazione non autorizzata o accesso accidentale/illecito):

- Notifica immediata al DPO (entro 24 ore dalla scoperta);
- Il DPO valuta il rischio e notifica al Garante Privacy entro 72 ore (art. 33 GDPR);

- Se la violazione presenta rischio elevato per i diritti degli interessati, comunicazione diretta agli stessi (art. 34 GDPR);
- Documentazione della violazione nel registro degli incidenti.

Art. 17) Regolamenti di sicurezza locali.

Le strutture dell'università devono dotarsi di direttive di sicurezza informatica, particolarizzate per le loro realtà. In queste direttive locali vengono specificate le responsabilità e le competenze in ambito di sicurezza informatica, oltre a tutte le ulteriori specifiche di sicurezza che ogni struttura sceglierà eventualmente di darsi. In questo ambito vanno specificati anche i provvedimenti, comminati a livello locale, in cui si incorre a seguito della violazione del regolamento locale e l'entità che si occupa di applicarli. Resta inteso che questi regolamenti locali devono uniformarsi a quelli generali di ateneo fissati in questo documento e devono essere approvati dall'area sistemi informativi prima di divenire operativi.

Art. 18) Acceptable Use Policy (AUP)

A tutti gli utenti della rete di ateneo deve essere reso noto il documento – AUP GARR- che riguarda i comportamenti da tenere nell'uso della rete e dei servizi dell'ateneo.

Regole per la cybersicurezza per i servizi informativi e server di Ateneo.

Art. 19) Regole Generali per la Struttura\Dipartimento

La struttura deve nominare un responsabile per ciascun sistema e per ciascun servizio applicativo; discrezionalmente, in funzione della natura dei sistemi e dei servizi, una stessa persona può essere nominata responsabile di più sistemi e/o servizi.
La struttura deve inoltre nominare al proprio interno un responsabile della sicurezza, eventualmente coincidente con uno dei responsabili di sistema o servizio, con il compito di:

- svolgere un'attività di supervisione e coordinamento tra i vari responsabili interni dei server e delle applicazioni in tema di sicurezza informatica;
- costituire l'interfaccia ufficiale della struttura nei confronti del gruppo sicurezza di rete per le tematiche connesse alla sicurezza dei sistemi e dei servizi offerti;
- costituire l'interfaccia ufficiale della struttura nei confronti dell'Incident Response Team per le emergenze connesse alla sicurezza di sistemi e servizi.

La struttura deve poi stilare un regolamento interno di sicurezza e, qualora lo ritenga opportuno, una carta dei servizi.
Il regolamento di sicurezza sarà un documento ad uso strettamente interno che conterrà le norme di sicurezza specifiche per i sistemi presenti, i servizi effettivamente erogati e il trattamento dei dati ospitati; non dovrà essere in disaccordo con il regolamento generale di ateneo e dovrà essere sottoposta all'approvazione del gruppo sicurezza di rete.
La carta dei servizi sarà invece un documento destinato alla diffusione e conterrà l'informativa generale per il pubblico con la descrizione dei servizi erogati, tempi e modi di fruizione del servizio, modulistica per le richieste di adesione al servizio, indirizzi di posta elettronica e i numeri di telefono del personale tecnico cui fare riferimento in caso di problemi nell'utilizzo di un servizio, etc.

Regole generali per gli amministratori di sistema

Art. 20) Criteri Generali

Gli amministratori di sistema devono garantire l'efficiente fruibilità del servizio minimizzando il rischio di usi impropri.
Essi devono garantire, per quanto possibile, la disponibilità del servizio secondo i tempi e i modi previsti dal regolamento interno di sicurezza e dalla eventuale carta dei servizi e operare in modo da minimizzare il rischio di:

- accessi non autorizzati al sistema;
- accessi non autorizzati ai dati;
- usi impropri del sistema che possano arrecare danno ad altri utenti del sistema, al sistema stesso o ad altri sistemi collegati alla rete dell'ateneo o alla Internet;
- usi impropri del sistema ovvero non attinenti alle attività istituzionali o comunque estranei alle finalità del trattamento dei dati, anche da parte degli utenti autorizzati.

Pertanto l'amministratore di sistema provvede alla gestione e manutenzione e patching di sistemi di elaborazione o delle loro componenti. Esso è individuato dal responsabile della Struttura.

La designazione degli amministratori di sistema avviene con atto formale scritto secondo il Provvedimento del Garante Privacy del 27/11/2008. L'elenco degli amministratori è conservato presso l'Area Sistemi Informativi e aggiornato costantemente. L'operato degli amministratori è oggetto di verifica annuale.
L'amministratore di sistema:

- assegna a ciascun utente una userid personale per l'accesso ai sistemi: una stessa userid non può essere assegnata a persone diverse neanche in tempi diversi, con l'eccezione degli userid di amministrazione se i sistemi operativi usati ammettono un solo livello di userid per l'amministrazione. Gli accessi degli amministratori devono comunque avvenire in prima istanza con la userid personale per consentire la tracciabilità delle sessioni.
- deve prontamente disattivare le userid degli utenti se questi perdono il diritto di accesso ai sistemi o se le userid rimangono inutilizzate per più di sei mesi.
- Le password di amministrazione dei sistemi dovranno essere:
    - cambiate periodicamente;
    - note esclusivamente agli amministratori;
    - diverse per ciascun sistema;
    - diverse da quelle già utilizzate in passato;
    - non coincidenti con le userid di amministrazione, neanche temporaneamente;
    - non banali e comunque di complessità adeguata al tipo di sistema;
    - non usate per scopi diversi dall'amministrazione dei sistemi.

Nessun applicativo deve far uso delle password di amministrazione, eventuali utilizzi specifici dovranno essere autorizzati dalla direzione generale, né aver bisogno dei privilegi di amministratore per il corretto funzionamento.
L'amministratore di sistema deve:

- installare i sistemi di protezione anti virus informatici di ateneo. Le applicazioni antivirus dovranno essere aggiornate in maniera automatica su base periodica; dovranno inoltre consentire la possibilità di aggiornamento manuale per far fronte ai casi di emergenza, come ad esempio in seguito a segnalazioni di diffusione di virus importanti.
- supervisionare eventuali accessi ai sistemi da parte di personale esterno, quale ad esempio fornitori di hardware o di servizi.

Qualora l'amministratore debba comunicare a consulenti esterni una o più password di amministrazione, di sistema o di base dati, le stesse dovranno essere sostituite prima e dopo il periodo di utilizzo.
Gli accessi con i privilegi di amministrazione devono di norma avvenire da postazioni interne alla struttura. Eventuali accessi dall'esterno dovranno essere ridotti al minimo indispensabile e con connessioni cifrate.

Art. 21) Sicurezza Fisica di Base dei Sistemi

Al fine di proteggere i sistemi, i locali che li ospitano dovranno possedere alcune caratteristiche indipendenti dal tipo di piattaforme hardware e dai sistemi operativi adottati.
Più precisamente, è opportuno che tali locali siano:

- dedicati ai server e preferibilmente presidiati;
- dotati di un sistema, meccanico o elettronico, di selezione degli accessi;
- dotati di un sistema di estinzione degli incendi;
- equipaggiati con dispositivi di stabilizzazione e continuità della tensione;

- climatizzati.

Eventuali interventi di qualsiasi natura (anche non informatica) in tali locali devono sempre avvenire in presenza di personale autorizzato.
In aggiunta a queste misure è consigliabile l'adozione di ulteriori accorgimenti per la restrizione degli accessi da implementare direttamente sui server, tra cui:

- l'impostazione di password per l'accesso al BIOS;
- il settaggio del BIOS in modo tale che l'avvio del sistema possa avvenire esclusivamente dal disco rigido di sistema.

Art. 22) Sicurezza Logica di Base dei Sistemi

Gli amministratori di sistema dovranno prevedere alcuni meccanismi per la sicurezza logica dei server che consentano di ridurre il rischio di esposizione dei dati e di accessi indesiderati ai server.

Art. 23) Protocolli e Socket TCP-UDP aperti sui sistemi

I server dovranno avere attivi solo i protocolli effettivamente necessari, tenendo presente che a livello di ateneo viene instradato esclusivamente il traffico IP; a livello IP dovranno essere attivi solo i protocolli strettamente necessari per il corretto funzionamento delle applicazioni.
A livello TCP e UDP dovranno essere disabilitate tutte le porte inutili e pericolose: dovranno essere aperte solo le porte strettamente necessarie per il funzionamento delle applicazioni.

Art. 24) Aggiornamento dei Sistemi Operativi e Patch di Sicurezza

Gli amministratori devono prestare attenzione agli alert in tema di sicurezza per i sistemi che gestiscono (con particolare riferimento alla vulnerabilità dei sistemi operativi e alle applicazioni di base), installare le patches non appena disponibili e valutare le azioni da intraprendere nel periodo intermedio in base al tipo e livello di rischio.
In ogni caso i sistemi operativi e i pacchetti di base dovranno essere regolarmente aggiornati, compatibilmente con le applicazioni installate sui sistemi.

Art. 25) Monitoraggio e Logging

I sistemi dovranno disporre di procedure per la registrazione dei messaggi di sistema e delle applicazioni di base attraverso meccanismi di logging per tutte le operazioni critiche.
I log di sistema devono essere analizzati regolarmente, preferibilmente per mezzo di meccanismi automatici di scansione in grado di generare allarmi a seguito di eventi rilevanti per la sicurezza del sistema.

Art. 26) Selezione e Controllo del Traffico Diretto ai Sistemi

I sistemi dovranno essere configurati in modo da accettare connessioni solo da parte dei client autorizzati e dagli amministratori.
Ove possibile, a livello di rete dovranno essere adottati sistemi per il controllo e la selezione del traffico di rete (traffic filtering, firewalling, etc.) previo accordo con il gruppo sicurezza di rete ed il servizio reti.
Nel caso in cui l'amministrazione dei server venga effettuata anche da remoto, la comunicazione tra il client e il server dovrà avvenire in maniera cifrata, il server dovrà essere configurato in modo

da non accettare chiamate dirette all'utente superuser e le chiamate dovranno essere limitate ad un gruppo identificato di indirizzi IP sorgenti.

Art. 27) Interventi sui Sistemi da Parte di Personale Esterno

Gli accessi ai sistemi da parte di personale esterno, fornitori di hardware o di servizi, dovranno avvenire sotto la supervisione degli amministratori.
Qualora si rendesse necessario comunicare una o più password di amministrazione, di sistema o di base dati, le stesse dovranno essere sostituite prima e dopo il periodo di utilizzo in modo da svincolarle da un eventuale logica di assegnazione adottata.
Nel caso di interventi che richiedano l'accesso per un periodo prolungato da parte di fornitori (es. upgrade, manutenzione, installazioni, test, etc.), le modalità di accesso dovranno essere definite a livello contrattuale.
Gli accessi con i privilegi di amministrazione devono di norma avvenire da postazioni interne alla struttura. Eventuali accessi dall'esterno dovranno essere ridotti al minimo indispensabile, ove possibile in maniera cifrata e in ogni caso valutati con estrema cautela.

Art. 28) Continuità del Servizio e Disaster Recovery

In caso di fermo, i servizi dovranno essere ripristinati nei tempi definiti dal regolamento interno di sicurezza e dalla eventuale carta dei servizi.
Per i fermi causati da guasti hardware è possibile stipulare contratti di manutenzione nei quali siano specificati i tempi di intervento oppure, qualora la struttura disponga di personale qualificato, dotarsi di parti di ricambio o sistemi alternativi che consentano alla struttura stessa di far fronte alle emergenze con mezzi propri nei tempi stabiliti.

Per i fermi di natura software o legati alla consistenza delle banche dati, dovranno essere implementati opportuni meccanismi di backup, le cui modalità e tempistiche dovranno essere specificate nel regolamento interno di sicurezza.

Regole per gli Applicativi – Gestione dei Servizi Centrali di Ateneo

Art. 29) Criteri Generali

Gli amministratori delle basi di dati e i gestori delle applicazioni devono garantire l'efficiente fruibilità dei servizi applicativi minimizzando il rischio di usi impropri.
Essi devono adoperarsi, per quanto possibile, a rendere disponibili dei servizi secondo i tempi e i modi previsti dal regolamento interno di sicurezza e dalla carta dei servizi e operare in modo da minimizzare il rischio di:

- accessi non autorizzati ai dati;
- usi impropri delle applicazioni che possano arrecare danno ad altri utenti del sistema, al sistema stesso o ad altri sistemi collegati alla rete dell'ateneo o alla Internet;
- usi illeciti dei dati o non attinenti alle attività istituzionali anche da parte degli utenti autorizzati.

Art. 30) Gestione degli Account per l'Accesso ai Servizi Applicativi

I gestori dei servizi applicativi devono assegnare a ciascun utente una userid personale: una stessa userid non può essere assegnata a persone diverse neanche in tempi diversi e non sono ammesse userid condivise per gruppi di utenza.
Nel caso di account per accessi espliciti a database valgono le stesse regole, con la sola eccezione della userid di superuser se il database ammette un solo livello di userid per l'amministrazione.
Gli accessi degli amministratori dei database e dei gestori delle applicazioni devono comunque avvenire in prima istanza con la userid personale per consentire la tracciabilità delle sessioni.
Gli amministratori e i gestori devono disattivare prontamente le userid degli utenti se questi perdono il diritto di accesso al servizio o se le userid rimangono inutilizzate per più di sei mesi.
Le password di amministrazione dei database e delle istanze dovranno essere:

- cambiate spesso;
- note esclusivamente agli amministratori;
- diverse per ciascuna base dati e istanza;
- diverse da quelle già utilizzate in passato;
- non coincidenti con le userid di amministrazione, neanche temporaneamente;
- non banali e comunque di complessità adeguata al tipo di dati custoditi;
- non usate per scopi diversi dall'amministrazione delle basi dati.

Art. 31) Accessi ai Servizi

Gli accessi ai servizi devono avvenire secondo le modalità e i tempi previsti dal regolamento interno di sicurezza e dalla eventuale carta dei servizi emessa dalla struttura.
I gestori delle applicazioni devono prendere misure opportune per assicurare la fruibilità del servizio agli utenti autorizzati e minimizzare i rischi di accesso da parte di altri utenti.

Art. 32) Attivazione di Nuovi Utenti

I gestori dei servizi applicativi devono predisporre sistemi di registrazione degli utenti con le informazioni minime necessarie per la trasmissione delle comunicazioni di servizio.
Al momento dell'attivazione, i gestori devono informare i nuovi utenti sulle modalità di accesso al servizio, fornire l'assistenza necessaria per la corretta procedura di connessione e informarli che, in caso di emergenza e per motivi di sicurezza, le userid possono essere disattivate anche senza preavviso.
I gestori devono inoltre informare gli utenti sulle responsabilità personali in caso di utilizzo da parte di terzi della propria password personale: tutti gli accessi effettuati con quella coppia userid-password saranno attribuiti a quell'utente anche se effettuati da altri.
Gli utenti devono pertanto essere invitati a:

- utilizzare i permessi di accesso esclusivamente per le finalità previste;
- non cedere la propria coppia userid-password a terzi;
- non lasciare in vista note o appunti che riportano userid e password;
- effettuare il logout dalle applicazioni e/o dal sistema oppure bloccare la workstation o attivare lo screen-saver con password in caso di allontanamento dalla stazione di lavoro;
- adottare password non banali

- sostituire periodicamente le password personali senza riutilizzare quelle già adottate in passato.

In relazione alla natura dei dati coinvolti, potrà essere chiesto agli utenti di firmare un modulo dal quale risulti che sono stati informati sulle regole di sicurezza da osservare.

Art. 33) Logging e Controllo

Le applicazioni devono prevedere un meccanismo di logging che consenta di tracciare le sessioni fino ad un livello di dettaglio ragionevole in virtù del tipo di applicazione.
I log devono essere regolarmente analizzati e conservati secondo quanto stabilito dal DPO in base alle finalità specifiche e nel rispetto del principio di minimizzazione (art. 5.1.c GDPR).
L'analisi dei log potrà avvenire manualmente ma è fortemente consigliata l'adozione di un sistema automatico in grado di segnalare tempestivamente situazioni anomale.

Art. 34) Statistiche sui Servizi Offerti

Fortemente consigliata è la predisposizione di un meccanismo di creazione e analisi delle statistiche di utilizzo di ciascun servizio erogato che permetta di valutare, ad esempio, il livello effettivo di accessi da parte dell'utenza, la banda di rete impegnata e il livello di carico imposto al sistema.
L'analisi delle statistiche in relazione ai dati storici, fornisce elementi oggettivi importanti ai fini del dimensionamento dei sistemi e dei servizi e consente di valutare l'opportunità di estendere o sospendere i servizi stessi. Inoltre consente di rilevare eventuali attività anomale che comportino, ad esempio, un aumento improvviso del volume di richieste, di carico di sistema o di traffico di rete.
I parametri da utilizzare per la creazione degli archivi statistici potranno essere specificati nel regolamento interno di sicurezza stilato della struttura.

Art. 35) Gestione Remota dei Servizi

Nel caso in cui l'amministrazione dei servizi venga effettuata anche da remoto, la comunicazione tra il client e il server dovrà avvenire in maniera cifrata, il servizio dovrà essere configurato in modo da non accettare chiamate dirette all'utente superuser e le chiamate dovranno essere limitate ad un gruppo identificato di indirizzi IP sorgenti.

Regole per l'accesso e l'utilizzo delle risorse informatiche di Ateneo

Art. 36) Utilizzo delle postazioni di lavoro

Nel caso in cui le postazioni di lavoro contengano dati personali, ad essi devono essere applicate tutte le prescrizioni di sicurezza previste dal Codice sul Trattamento dei dati personali (Regolamento U.E. 2016/679 del 27 aprile 2016).
È consentito l'uso di programmi esclusivamente nel pieno rispetto degli obblighi imposti dalla vigente normativa sulla tutela giuridica del software e del diritto d'autore.
In particolare:

- l'utente è responsabile per le attività svolte nella Rete dati di Ateneo;
- l'utente è responsabile per eventuali difformità riscontrate sulle apparecchiature assegnate;
- la modifica dell'indirizzo IP configurato (in maniera dinamica o manualmente) sull'host assegnato è espressamente vietata;
- utilizzare i permessi di accesso esclusivamente per le finalità previste;
- l'utente è tenuto ad effettuare il logout dalle applicazioni e/o dal sistema oppure bloccare la workstation o attivare lo screen-saver con password in caso di allontanamento dalla stazione di lavoro;
- l'utente è tenuto ad adottare password con il seguente criterio di conformità:
    - non devono contenere parti significative del nome di account o del nome dell'utente;
    - devono essere composte almeno da 8 caratteri;
    - devono contenere caratteri appartenenti a tre delle quattro categorie seguenti:
        - lettere maiuscole (dalla A alla Z)
        - lettere minuscole (dalla a alla z)
        - i primi 10 numeri di base (da 0 a 9)
        - caratteri non alfabetici (ad esempio, !, $, #, %)
- l'utente è responsabile per la protezione dei dati utilizzati e/o memorizzati nei sistemi a cui ha accesso ed è tenuto ad adottare tutte le misure necessarie ai sensi della normativa vigente e del "Regolamento per la sicurezza informatica" emanato dall'Ateneo;
- la responsabilità dei contenuti prodotti e diffusi attraverso la rete di Ateneo è dell'utente che li produce e li diffonde;
- l'utente è tenuto a segnalare all'Area Sistemi Informativi o al referente di struttura ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;
- l'utente è tenuto ad aggiornarsi su direttive di sicurezza o comportamenti da adottare periodicamente diffusi dall'Area Sistemi Informativi attraverso il proprio sito o per mezzo di comunicazioni per posta elettronica in particolare, se l'account utilizzato ha diritti amministrativi sulla postazione di lavoro, è tenuto a installare e mantenere aggiornato l'eventuale software antivirus sull'Host affidato. Tale antivirus deve necessariamente essere quello acquistato dall'Ateneo o dal dipartimento per tale scopo.
- l'utente è tenuto ad impostare ed attivare il blocco con password del sistema operativo in caso di allontanamento anche temporaneo dalla postazione di lavoro, al fine di evitare di lasciare la risorsa informatica incustodita;

- l'utente è tenuto a spegnere il proprio host al termine dell'attività lavorativa prima di allontanarsi dalla postazione di lavoro salvo motivate esigenze di servizio/istituzionali.

È vietato:

- cedere la propria coppia userid-password a terzi;
- lasciare in vista note o appunti che riportano userid e password;
- utilizzare le risorse hardware e software fornite dall'Ateneo, per conservare file di natura personale per scopi non strettamente correlati con le finalità lavorative;
- accedere alla Rete Dati di Ateneo per conseguire l'accesso non autorizzato a risorse di rete interne od esterne all'Università;
- fornire il servizio di connettività di rete a soggetti non autorizzati all'accesso alla Rete di Ateneo;
- usare false identità, l'anonimato o servirsi di risorse che consentono di restare anonimi; ove l'utente contravvenga a tale divieto il Servizio Reti provvederà ad impedire l'accesso alla Rete;
- violare obblighi in materia di copyright, licenze d'uso di software;
- svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, danneggino o restringano l'utilizzabilità o le prestazioni della Rete di Ateneo;
- manomettere in qualsiasi modo le apparecchiature e le strutture informatiche ed elettroniche dell'Ateneo;
- violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni (software, database, ecc.), intercettare, tentare di intercettare o accedere a dati in transito sulla Rete Dati d'Ateneo, dei quali non si è destinatari specifici;
- distruggere o tentare di distruggere, danneggiare o tentare di danneggiare, intercettare o tentare di intercettare o accedere o tentare di accedere senza autorizzazione alla posta elettronica o ai dati di altri utenti o di terzi, usare, intercettare o diffondere o tentare di intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri utenti o di terzi, e in generale commettere o tentare di commettere attività che violino la riservatezza di altri utenti o di terzi, così come tutelata dalle norme civili, penali e amministrative applicabili;
- diffondere immagini, dati o altro materiale potenzialmente offensivo, diffamatorio o dal contenuto osceno;
- utilizzare la Rete dati di Ateneo e i servizi da essa offerti a scopi commerciali e per propaganda politica o elettorale;
- trasferire materiale in violazione delle norme sulla proprietà intellettuale, mediante programmi di tipo "Peer to Peer";
- trasferire attraverso la rete documenti (filmati, fotografie, musica o altri documenti multimediali) ad uso strettamente personale anche se muniti di regolare diritto di utilizzo, non inerente la normale attività lavorativa.
- cablare o collegare risorse informatiche ai punti rete senza l'autorizzazione del Servizio Reti;
- connettere un Host, contemporaneamente, alla rete d'Ateneo e ad altra rete (es. ADSL, GPRS);

- copiare (a meno che la licenza d'uso non lo consenta) e/o utilizzare i programmi messi a disposizione dall'Amministrazione per installazioni esterne;

L'Ateneo si riserva la facoltà di procedere tramite l'Area sistemi Informativi alla rimozione di ogni file o applicazione, anche dotati di regolare licenza d'uso, che riterrà essere pericolosi per la sicurezza del sistema informatico o causa di malfunzionamenti per l'host o per la rete dati, ovvero acquisiti o installati in violazione del presente Regolamento.

Art. 37) Utilizzo della rete da parte degli utenti

Ogni utilizzatore della rete è tenuto in ogni caso ad adottare le necessarie misure per non interferire nel corretto funzionamento delle comunicazioni e per garantire l'integrità dei sistemi e l'accesso alle risorse da parte degli altri utenti.
Non è consentito:

- navigare in siti non pertinenti rispetto alle specifiche necessità di lavoro o di studio;
- il download con procedure non legali di opere protette dal diritto d'autore e da altri diritti connessi al suo esercizio quali opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro, alla cinematografia, qualunque ne sia il modo o la forma di espressione;
- il download con procedure non legali di programmi per elaboratore tutelati ai sensi della convenzione sulla protezione delle opere letterarie e artistiche, nonché le banche di dati che per scelta o la disposizione del materiale costituiscono una creazione dell'autore;
- la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- qualsivoglia attività vietata dalle leggi vigenti.

Le copie di sicurezza delle registrazioni del traffico (file di log) degli accessi e/o delle applicazioni, contenenti la data, l'ora e gli estremi identificativi dell'utilizzatore, effettuate per fini strettamente correlati alla gestione tecnica del servizio sono conservate secondo le norme vigenti.

Art. 38) Utilizzo di software

Qualsiasi software, a qualsiasi titolo acquisito o realizzato dall'Ateneo, deve essere protetto da distruzioni o perdite anche accidentali, alterazioni, usi illeciti e divulgazioni non autorizzate.
Qualsiasi software non espressamente rilasciato con strumenti finalizzati alla diffusione pubblica è da intendersi riservato.
La riproduzione, installazione, duplicazione, distribuzione e ogni altra forma di utilizzo dei programmi per elaboratore, in quanto opere dell'ingegno tutelate dalla legge, può avvenire lecitamente solo nel rispetto dei diritti d'autore e delle licenze d'uso.
Si precisa che:

- l'Ateneo non fornisce alcuna garanzia su software distribuiti gratuitamente e in particolare non garantisce la loro adeguatezza e fruibilità per scopi specifici;
- in nessun caso l'Ateneo potrà essere ritenuto responsabile per danni diretti, indiretti o derivanti dall'uso dei software distribuiti gratuitamente o dai risultati da essi forniti; in particolare non potrà essere ritenuto responsabile per eventuali ritardi, inadempienze,

perdita di dati e danni economici derivanti o in qualche modo collegati all'uso di tali software od ai risultati da essi forniti.

Art. 39) Controllo e uso dei dati di accesso e di utilizzo dei log

L'Ateneo utilizza i dati relativi agli accessi ai propri sistemi informatici, applicazioni, programmi, dati e transazioni da parte dei componenti la comunità universitaria:

- per motivi di sicurezza;
- per la corretta gestione degli stessi dati e delle informazioni;
- per la corretta gestione delle risorse informatiche;
- per le statistiche d'uso relative ai sistemi informatici;
- per le attività relative a modifiche tecniche/operative.

Tali accessi avverranno in conformità con le disposizioni del Garante per la Protezione dei Dati Personali e in particolare delle "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n 300 del 24 dicembre 2008)".
Nel rispetto delle previsioni di cui all'art. 4 della L. 300/70, i dati raccolti relativi agli accessi ai servizi informatici saranno utilizzati garantendo la protezione dei dati personali, in conformità con la disciplina legislativa in materia e nella tutela di interessi economici e commerciali vivi, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali secondo le specifiche norme nazionali e internazionali vigenti in materia.

Art. 40) Sanzioni

A fronte di violazioni accertate delle regole stabilite dal presente regolamento, al fine di evitare ripercussioni sulla Rete Telematica e sui servizi, i responsabili/referenti informatici di Ateneo e dei Dipartimenti, possono disporre la sospensione temporanea delle credenziali di identità digitale che consentono la fruizione dei servizi di Ateneo.
Detta sospensione deve essere comunicata immediatamente all'interessato e all'Area Sistemi Informativi che può sospendere o disattivare in qualsiasi momento: l'identità digitale, apparati ritenuti non conformi o pericolosi ai fini della sicurezza, disconnettere un host dalla rete, senza necessità di preventivo avviso; qualora la disattivazione sia necessaria all'integrità o al funzionamento della Rete di Ateneo, oppure qualora vi sia evidenza che l'utente abbia violato il presente Regolamento.
L'Area Sistemi Informativi si riserva la possibilità di erogare assistenza in caso di violazione del presente regolamento, ferma restando la segnalazione agli Organi competenti di Ateneo e le eventuali applicazioni di sanzioni disciplinari, civili per danni e penali.