Norme di Attuazione del Regolamento per l'utilizzo della posta elettronica e internet

Indice

Art. 1 - Glossario 1
Art. 2 - Oggetto e ambito di applicazione 2
Art. 3 - Norme Generali di Regolamentazione Accesso alla Rete di Ateneo 3
Art. 4 - I Soggetti con Diritto di Accesso alla Rete ed ai Servizi di Ateneo 4
Art. 5 - Processo e Gestione Accreditamento Utenti 5
Art. 6 - Ruoli 5
Art. 7 - Formato e Regole delle Credenziali GIA 7
Art. 8 - Classificazione dei Dati 7
Art. 9 - Classificazione dei Luoghi di Accesso alla Rete Univr 8
Art. 10 - Topologia della Rete dell'Università degli Studi di Verona 8
Art. 11 - Architettura di Sistema per l'Accesso alla Rete dell'Università degli Studi di Verona 9
Art. 12 - Architettura di Sicurezza per Accessi dall'esterno 10
Art. 13 - I Servizi di Rete 10
Art. 14 - Regole di Utilizzo di Servizi di Rete con Accesso tramite le Federazioni EDUROAM/IDEM del Consorzio GARR 11
Art. 15 - Posta Elettronica @univr.it 12
Art. 16 - Gestione Server in Ateneo 14
Art. 17 - Titolarità del dominio DNS univr.it 15
Art. 18 - Gestione dei domini di terzo livello interni ad univr.it 15
Art. 19 - Domini di secondo livello differenti da "univr.it" 16
Art. 20 - Domini di quarto livello. Modalità di richiesta e durata delle registrazioni 16
Art. 21 - Portale di Ateneo e Siti Web 17
Art. 22 - Rilevazione e Gestione degli Incidenti per la Sicurezza 17
Art. 23 - Monitoraggio e Controllo 18
Art. 24 - Memorizzazione dei File di Log 18

Art. 1 - Glossario

Si definiscono, per gli scopi del presente documento, i seguenti elementi:

➡**Accesso con login**: l'accesso alla rete di Ateneo o a suoi servizi mediante una coppia di credenziali composta da username e password GIA;

➡**Applicazioni ad alto impatto sulla rete**: Applicazioni che richiedano una significativa disponibilità di banda sulla dorsale di Ateneo (es. videoconferenza su IP, multimedialità, realtà virtuale, etc.);

➡**Client**: Un host che utilizza un servizio di rete;

➡**Dispositivo di rete**: Router, Switch, Access Point Wireless o qualunque altra apparecchiatura che permetta di estendere la rete di Ateneo;

➡**GARR** (Gestione Ampliamento Rete Ricerca) è il Consorzio che fornisce la connettività Internet agli Atenei Italiani. Ha lo scopo di "fornire ai ricercatori servizi indipendenti dalla collocazione geografica, favorendo il coordinamento e la collaborazione nelle attività di ricerca nazionali ed internazionali e la diffusione e sperimentazione di tecnologie avanzate e nuovi servizi".

➡**EDUROAM (EDUcation ROAMing):** Federazione del Consorzio GARR dove gli utenti delle istituzioni che aderiscono alla federazione hanno la possibilità di usufruire gratuitamente di una connessione Internet wireless presso tutte le sedi delle organizzazioni aderenti alla federazione.

➡**Host**: Un computer connesso alla rete;

➡**IDEM (IDEntity Management per l'accesso federato)**: E' un servizio di autenticazione che permettere agli utenti degli Enti Accademici e di Ricerca che hanno scelto di aderire alla federazione IDEM di utilizzare per l'accesso le proprie credenziali (quelle utilizzate nella propria istituzione) per accedere a risorse federate di tutte le istituzioni che partecipano al progetto.

➡**Indirizzi pubblici (IP Pubblici)**: L'insieme di tutti gli indirizzi pubblici registrati GARR per l'Università degli Studi di Verona [157.27.0.0/16];

➡**Internet**: L'insieme mondiale di tutte le reti interconnesse tra di loro. Internet è per definizione untrusted e nell'ambito delle Norme di Attuazione coincide con tutte le reti diverse da quelle dell'Ateneo;

➡**Intranet**: La rete di trasmissione dati che interconnette tutti gli insediamenti dell'Ateneo con piano di numerazione privato 10.0.0.0/8 e inoltre per il Servizio SSLVPN i piani di numerazione 157.27.8.0/24;

➡**NAC:** E' un Servizio di autenticazione su rete cablata (wired) che utilizza un insieme di protocolli più o meno proprietari per regolarizzare l'accesso alla rete cablata dell'Università di Verona solo agli utenti con credenziali GIA.

➡**Rete di backbone**: l'insieme delle infrastrutture di rete, composto da dispositivi di rete, fibre ottiche, cavi, collegamenti diretti numerici, xDSL, in grado di interconnettere sia a livello fisico che a livello di rete tutti gli insediamenti presenti nell'Ateneo;

➡**Rete di Ateneo**: l'insieme di tutti le reti e i dispositivi descritti nelle Norme di Attuazione;

➡**Server Internet**: un Server di rete accessibile da Internet;

➡**Server Intranet**: un Server di rete visibile solo all'interno della rete intranet;

➡**SSL VPN** (**S**ecure **S**ockets **L**ayer **V**irtual **P**rivate **N**etwork): La rete privata virtuale (VPN) che fornisce un meccanismo di comunicazione protetta per i dati e le informazioni trasmesse.

Art. 2 - Oggetto e ambito di applicazione

Il presente documento, di seguito indicato con il termine Norme di Attuazione, contiene la descrizione dei servizi di posta elettronica e di accesso ad Internet nonché le norme tecniche per l'attuazione del "Regolamento per l'utilizzo della posta elettronica e internet" dell'Ateneo di

Verona, di seguito indicato con il termine Regolamento, e ha quindi lo stesso ambito di applicazione.

Art. 3 - Norme Generali di Regolamentazione Accesso alla Rete di Ateneo

L'utente che utilizza dispositivi elettronici dotati di connettività (personal computer fissi e portatili, dispositivi mobili come smartphone, tablet, palmari e lettori di ebook, etc …) in grado di accedere - mediante rete cablata o wireless - alla Rete di Ateneo deve attenersi alle normative vigenti in materia di sicurezza informatica e tutela della privacy, alle apposite regole di accesso e di utilizzo del Consortium GARR (Acceptable Use Policy - AUP), al Regolamento e alle presenti norme di attuazione del Regolamento.
In base alle Acceptable Use Policy del GARR, l'utilizzo è consentito esclusivamente per attività istituzionali, ovvero "l'attività di ricerca, la didattica, le funzioni amministrative".
L'utente è tenuto a mantenere i propri dispositivi aggiornati, sicuri ed efficienti. A questo scopo, dovranno essere applicati i più recenti aggiornamenti del sistema operativo ed adottati strumenti software in grado di proteggere il sistema da eventuale codice malevolo.
L'accesso alla rete dati, ed ai relativi servizi ad essa associati, è consentito all'utente solo mediante l'utilizzo delle credenziali GIA.
Tali credenziali sono strettamente personali e pertanto non cedibili; la responsabilità del loro utilizzo fa capo direttamente all'utente ad esse associato: l'Ateneo non si assume alcuna responsabilità nel caso in cui queste siano utilizzate impropriamente.
Qualora l'utente avesse il sospetto che le proprie credenziali siano state compromesse, dovrà tempestivamente procedere alla modifica della password o, se non più possibile, segnalare immediatamente l'accaduto all'Area Supporto.
L'utente si impegna ad utilizzare i Servizi di Rete per le finalità sovraesposte e si impegna altresì a non utilizzare la rete universitaria per fini diversi da quelli istituzionali.
E' espressamente vietato:

- collegare di propria iniziativa apparati attivi di rete, come ad esempio access point wireless, switch, router, firewall, etc.., indipendentemente dal livello di sicurezza che questi sono in grado di offrire;
- implementare servizi DHCP e DNS alternativi a quelli già erogati dall'Ateneo.
- configurare di propria iniziativa dispositivi per distribuire in rete protocolli quali WINS, FTP, TFTP, SMTP, SMTPS, POP3, POP3S, IMAP, IMAPS, etc…se non previa accordi con il personale tecnico della struttura di riferimento ed autorizzazione espressa dal personale dell'area reti .
- trasmettere frame di rete difformi dallo standard Ethernet II, come ad esempio IEEE 802.3, IEEE 802.2 LLC o IEEE 802.2 SNAP, ed abilitare la trasmissione di protocolli come IPX/SPX, Appletalk, Ethertalk, ecc.
- intraprendere azioni di scansione della rete o attacchi alla sicurezza, in quanto queste potrebbero condurre all'applicazione di contromisure che potrebbero impattare sulla regolare erogazione del servizio di connettività;
- configurare manualmente le impostazioni relative all'indirizzo IP del proprio dispositivo: l'impostazione manuale di questi parametri è prevista solo se espressamente concordata con il personale informatico della struttura di riferimento ed espressamente autorizzata dall'Area Reti, e si applica solamente a dispositivi che attendono a particolari funzioni e che saranno volta per volta singolarmente oggetto di valutazione;
- distribuire in rete materiali illegale e/o strumenti in violazione della leggi sul diritto di autore e sulla proprietà intellettuale e industriale: lo scambio di materiale protetto dal diritto d'autore è vietato per legge e soggetto a sanzioni anche di natura penale; in caso di

rilevamento di comportamenti illegali, l'Università di Verona procederà al richiamo formale dell'Utente e metterà a disposizione delle autorità che ne facessero richiesta tutta la relativa documentazione;
- utilizzare la rete per l'invio di materiale pubblicitario e/o promozionale o per comunicazioni massive dirette a gruppi di soggetti, siano essi afferenti o meno all'Ateneo;
- diffondere in rete informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, razzista, diffamatorio ed offensivo;

L'Ateneo non si assume alcuna responsabilità in merito ai dati contenuti nei dispositivi personali degli Utenti. In caso di aggressione da software malevoli o di attacco da parte di malintenzionati che dovessero, in qualsiasi maniera, danneggiare l'operatività dei suddetti o i dati in essi contenuti, l'Utente non potrà in alcun modo rivalersi sull'Università di Verona.

L'Utente sarà responsabile per eventuali danni, turbative e violazioni effettuati in rete e/o a terzi in violazione della legge o dei regolamenti vigenti in materia di privacy e riservatezza dei dati.

Art. 4 - I Soggetti con Diritto di Accesso alla Rete ed ai Servizi di Ateneo

In conformità all'Art. 11 del Regolamento, sono da considerarsi autorizzati all'accesso alla rete dati di Ateneo: i dipendenti e studenti dell'Ateneo e tutti coloro che hanno un rapporto di lavoro, di collaborazione, di ricerca o di didattica, anche a tempo determinato, o che sono interessati alla fruizione di contenuti bibliotecari, purché riconosciuti nominalmente da una Delibera di un Organo del Centro di Responsabilità (CdR) con il quale l'Utente ha relazioni o da altro Organo dell'Ateneo; oppure da attestazione di Docenti, Ricercatori e Dirigenti: in questi ultimi casi unicamente per rapporti di breve durata (per esempio, visiting professor).

Ai soggetti autorizzati sono fornite opportune credenziali di accesso e autenticazione, rilasciate dai soggetti di cui al paragrafo precedente, fermo restando che al momento dell'offerta delle credenziali di accesso e autenticazione, è necessario acquisire i dati dell'Utente conformemente a quanto previsto dalle norme vigenti.

Al personale accademico e tecnico amministrativo che interrompano il rapporto con l'Ateneo viene concesso un ulteriore periodo di 5 anni, dalla cessazione del rapporto, che prevede la conservazione della casella di posta elettronica, l'accesso ad Internet tramite rete cablata e Wi-Fi, i servizi ad essa correlati come la VPN e l'accesso a riviste e banche dati elettroniche oltre ai privilegi necessari per l'accesso. Entro il termine di tale periodo il personale dovrà provvedere, tramite le funzioni del sistema di posta elettronica, a reindirizzare la posta in arrivo e a impostare un messaggio di risposta automatica che comunichi ai corrispondenti le informazioni necessarie per l'aggiornamento del contatto.

Agli studenti che terminano il loro rapporto con l'Università viene concesso un ulteriore periodo di 5 anni, che prevede la conservazione della casella di posta elettronica e i privilegi necessari per l'accesso alla stessa. Per i primi due anni si mantiene anche la possibilità di accesso ad Internet, tramite rete cablata e Wi-Fi, i servizi ad essa correlati come la VPN e l'accesso a riviste e banche dati elettroniche oltre ai privilegi necessari per l'accesso. Entro il termine dei 5 anni lo studente dovrà provvedere autonomamente, tramite le funzioni del sistema postale, a reindirizzare la posta in

arrivo e a impostare un messaggio di risposta automatica che comunichi ai corrispondenti le informazioni necessarie per l'aggiornamento del contatto.

Art. 5 - Processo e Gestione Accreditamento Utenti

Il processo di accreditamento viene avviato quando, nell'ambito di una struttura organizzativa di Amministrazione Centrale o di Struttura Decentrata nasce l'esigenza di accreditare all'accesso alle risorse informatiche da parte di soggetti con diritto di accesso.

Il processo è svolto direttamente dal Responsabile della Privacy del CdR ai sensi del D.lgs. 196/2003 (ADM-RSP-CDR) oppure dal Gestore GIA (ADM-GES-GIA) a seguito di assegnazione di incarico da parte del Responsabile oppure da personale incaricato e delegato al ruolo di Responsabile della Gestione Anagrafica del Personale (ADM-RSP-GAP) in servizio presso la segreteria della struttura organizzativa.

Il Responsabile che svolge il processo provvede all'identificazione dell'Utente e all'accertamento dei requisiti necessari per l'accreditamento e, di fronte ad esito positivo, crea o aggiorna il profilo anagrafico in accordo.

L'Amministrazione quindi provvede all'accreditamento informatico attraverso il sistema di Identity Management denominato GIA il quale permette la gestione automatica del ciclo di vita (creazione, modifica, disabilitazione) delle identità e delle credenziali elettroniche degli utenti.

Il processo di accreditamento degli utenti si basa sulla integrazione tra Risorse Autorevoli e Risorse "Provisionate" (risorse che sono destinatarie di sincronizzazione delle credenziali) e su deleghe amministrative garantite dal sistema GIA.

Gli Utenti (persone) sono classificati sulla base dell'appartenenza a Classi e Sottoclassi di Identità. I Ruoli nella gestione delle identità e le Responsabilità ai sensi del D.lgs. 196/2003 sono definiti sulla base del posizione organizzativa e delle attribuzioni formali conseguenti sia di carattere collettivo che individuale.

Di seguito, Art. 5, sono riportate in forma tabellare le informazioni relative ai Ruoli Amministrativi UniVR–GIA delle entità coinvolte nel processo di accreditamento e di gestione delle credenziali e alle relative responsabilità.

Art. 6 - Ruoli

Le **Classi di Identità** relativi ai Ruoli Utente UniVR–GIA gestiti nel processo di accreditamento sono le seguenti:

➡**Studenti** [Iscritti, Specializzandi, Post-Lauream, Alumni, In Limbo]: Per questa classe le Risorse Autorevoli sono ESSE3 del Cineca (studenti Iscritti, In limbo, Alumni) e fino al 2011 è la vista GAS (Gestione Anagrafica Studenti) sul gestionale di backoffice SEGRE di UniVR (studenti Specializzandi e Post-Lauream).

➡**Personale** [Accademici (Strutturati/Non Strutturati), Dottorandi, Tecnico-Amministrativi (Strutturati/Non Strutturati): Per questa classe la Risorsa Autorevole è la vista GAP (Gestione Anagrafica Personale) sul gestionale di backoffice dbERW che gestisce i contenuti del Web Integrato di Ateneo nonché tutte le informazioni sull'offerta formativa e l'organizzazione.

➡**Esterni** [Consulenti&Fornitori, Ospedalieri, 150H]: Per questa classe la Risorsa Autorevole è la vista GAE (Gestione Anagrafica Esterni) sul gestionale di backoffice dbERW che gestisce i contenuti del Web Integrato di Ateneo che gestisce tutte le informazioni sull'offerta formativa e l'organizzazione.

➡**Frequentatori** [Ospiti, Congressisti, Studenti ospiti, Studenti frequentatori, Frequentatori biblioteca]: Per queste classe la Risorsa Autorevole è il sistema GIA stesso attraverso funzionalità delegate a Docenti, Responsabili di Anagrafica e Operatori di Biblioteca.

Si definiscono, per gli scopi del presente regolamento, nel loro **Ruolo Amministrativo** i seguenti soggetti:

➡**Ateneo**: l'Università degli Studi di Verona;

➡**Tecnico di Dipartimento**: Questo ruolo individua le responsabilità di verifica dell'identità ed attivazione del password reset per tutte le identità associabili alle Strutture Decentrate (in Fase 1 sono esclusi i Centri).

➡**Tecnico SIA**: Questo ruolo individua le responsabilità di verifica dell'identità ed attivazione del password reset per tutte le identità associabili alle Amministrazioni Centrali (in Fase 1 sono esclusi gli Organi e le Biblioteche).

➡**Responsabile della Privacy del Centro di Responsabilità (CdR)**: I responsabili dei CdR (Struttura organizzativa di UniVR) avente Responsabilità ai fini del D.lgs. 196/2003 sono coinvolti in alcuni processi come quello relativo alla richiesta di accesso per un ospite o l'estensione dei privilegi di accesso.

➡**Gestore GIA**: Questo ruolo consente l'amministrazione di tutte le funzionalità del sistema GIA, ovvero corrisponde ad una sorta di super-utente.

➡**Direzione GIA**: A questo ruolo è associato un sottoinsieme delle capacità amministrative del GIA, soprattutto riferite alla gestione dei report e statistiche.

➡**Responsabile Gestione Privilegi**: Questo ruolo individua genericamente l'autorità nel fornire o revocare l'assegnazione di privilegi di accesso ad un particolare utente e dipende dal tipo di privilegio considerato.
Ad esempio nel caso del privilegio di accesso all'applicativo CIA (Contabilità Integrata di Ateneo), tale autorità sarà assegnata nell'ambito della Direzione Finanza e Contabilità. Nel GIA il ruolo in oggetto viene specializzato nelle seguenti responsabilità "Gestore Servizi FCO", "Gestore Servizi Protocollo" e "Gestore Servizi SIA".

➡**Responsabile Anagrafica Personale**: Responsabile Gestione Anagrafica Personale (definisce il ruolo amministrativo della figura professionale che assume la responsabilità della gestione dei dati anagrafici del Personale sia in fase di creazione che di modifica (ad esempio delle date di inizio/fine rapporto).

➡**Responsabile Anagrafica Esterni**: Responsabile Gestione Anagrafica Esterni (definisce il ruolo amministrativo della figura professionale che assume la responsabilità della gestione dei dati anagrafici degli Esterni sia in fase di creazione che di modifica (ad esempio delle date di inizio/fine rapporto).

➡**Responsabile Anagrafica Studenti**: Responsabile Gestione Anagrafica Studenti (definisce il ruolo amministrativo della figura professionale che assume la responsabilità della gestione dei dati anagrafici degli Studenti sia in fase di creazione che di modifica (ad esempio delle date di inizio/fine rapporto).

➡**Area Informatica**: E' l'Area che progetta, implementa e gestisce tutti i servizi, i server, i sistemi e le reti dell'Ateneo. Può avvalersi di gruppi di lavoro composti da esperti del settore, per specifici progetti finalizzati alla sperimentazione di soluzioni e innovazioni tecniche da proporre agli Organi Accademici.

Art. 7 - Formato e Regole delle Credenziali GIA

Il sistema GIA allo stato attuale prevede la realizzazione del cosiddetto singolo login via UserID/Password, ovvero l'utilizzo di credenziali uniche per l'accesso a tutte le Risorse Provisionate.

Le politiche relative agli accountID sono differenziate a seconda della Risorse Autorevole che ne effettua il provisioning:

➡**Personale Interno ed Esterno**: accountID di 8 caratteri costituito dei primi 6 caratteri del Codice Fiscale concatenati con 2 cifre numeriche casuali;

➡**Studenti Iscritti**: accountID di 8 caratteri costituito dalle lettere ID concatenate con 3 cifre numeriche casuale e 3 lettere casuali;

➡**Studenti post-lauream:** accountID di 8 caratteri costituito dalle lettere VR concatenate con 6 cifre numeriche progressive;

➡**Frequentatori**: accountID costituito da una parte letterale determinata dalla sottoclasse di identità e da una parte numerica progressiva.

I criteri di robustezza della password previsti nel sistema GIA sono:

➡**Lunghezza minima**: 8

➡**Lunghezza massima**: 32

➡**Minimo numerici**: 1

➡**Minimo maiuscoli**: 1

➡**Minimo minuscoli**: 1

➡**Minimo speciali**: 1

E' prevista l'introduzione della scadenza della password a 6 mesi per il Personale Interno.

Per la gestione della password di primo accesso e della password dimenticata sono previste due modalità alternative: la prima prevede l'intervento del supporto tecnico nelle procedure di identificazione e approvazione, la seconda è compiuta in modalità autonoma ed è disponibile agli utenti che abbiano preventivamente registrato in GIA un indirizzo email privato.

Art. 8 - Classificazione dei Dati

Si definiscono, per gli scopi del presente regolamento, le seguenti tipologie di dati:

➡**Dati personali**: Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

➡**Dati sensibili**: I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati,

associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

➡**Dati scientifici**: le informazioni riguardanti l'attività didattica e di ricerca dell'Ateneo;

➡**Dati amministrativi**: Informazioni e comunicazioni riguardanti tutto ciò che concerne l'amministrazione dell'Ateneo per il conseguimento dei propri fini istituzionali;

➡**Dati riservati**: Dati amministrativi a uso interno o coperti dal segreto d'ufficio;

➡**Dati critici**: Le informazioni, le applicazioni informatiche o i sistemi operativi relativi agli host fornitori di servizi di rete e a quelli che possono compromettere significativamente la sicurezza della rete di Ateneo.

Art. 9 - Classificazione dei Luoghi di Accesso alla Rete Univr

Si definiscono, per gli scopi delle presenti Norme di Attuazione, i seguenti luoghi di accesso:

➡**Uffici e Studi**: Luoghi riservati al personale strutturato dell'Ateneo ed eventualmente a collaboratori temporanei;

➡**Laboratori Didattici**: Luoghi dedicati alle esercitazioni didattiche;

➡**Locali Tecnici**: spazi chiusi con presenza esclusiva di apparati di rete;

➡**Laboratori di Ricerca**: Luoghi dedicati all'attività di ricerca;

➡**Biblioteche**: Luoghi di consultazione di materiale librario, cartaceo o digitale;

➡**Spazi Comuni**: Luoghi di passaggio o di incontro dove siano presenti punti di accesso sia cablati che tramite Servizio Wireless alla rete di Ateneo.

Art. 10 - Topologia della Rete dell'Università degli Studi di Verona

La Rete dell'Università di Verona connette la sede centrale dove è ubicato il Centro Servizi collegato ad Internet tramite il Consorzio GARR con un doppio collegamento in fibra della velocità di 1Gbps ciascuna.

L'infrastruttura collega le singole sedi al Centro Servizi, il quale si fa carico di garantire la connettività verso la rete Internet.

Le sedi collegate alla rete di Ateneo sono suddivise in base alla tipologia di connessione e sono le seguenti:

Dorsali

➡Istituti Biologici, Strada le Grazie 8, Verona con collegamento ad 1 Gbps;

➡Dipartimento di Scienze Giuridiche, Via Montanari 9, Verona con collegamento ad 1 Gbps;

➡Dipartimento di Scienze della Vita e della Riproduzione, Via Casorati 43, Verona con collegamento a 100 Mbps;

➡l'Istituto Ex- Orsoline in Via Paradiso 6, Verona con collegamento a 100 Mbps;

➡Dipartimento di Scienze Economiche, Via San Cristoforo 4, Verona con collegamento a 100 Mbps;

➡Ospedale Civico di Borgo Trento, Verona con collegamento a 100 Mbps;

Collegamenti in ambito metropolitano

➡Palazzo Giusti, Via Giardino Giusti 2, Verona con collegamento a 10 Mbps;

➡Distaccamento di Economia, Via del Fante 5, Verona con collegamento a 10 Mbps;

➡C.d.L. in Scienze del Servizio Sociale, Via Filippini 18, Verona con collegamento a 4 Mbps.

➡

Collegamenti in ambito extraurbano

➡Polo Universitario Scientifico Didattico "Studi sull'Impresa", Viale Margherita 87, 36100 Vicenza con collegamento a 8 Mbps;

➡Centro di Ricerca Sport Montagna Salute (Ce.Ri.S.M.), Via Matteo del Ben 5/b, Rovereto (TN) con collegamento a 4 Mbps;

➡C.d.L. in Scienze e Tecnologie Viticole ed Enologiche, Villa Lebrecht, San Floriano di Valpolicella (VR) con collegamento a 4 Mbps;

➡Sede di Canazei, Via de Sorapera, 25-27, Alba di Canazei (TN) con collegamento a 4 Mbps;

➡C.d.L. in Infermieristica, Via Carlo Giannella 1, Legnago (VR) con collegamento a 2 Mbps;

➡C.d.L. in Infermieristica, Contrà San Bortolo 85, Vicenza con collegamento a 2 Mbps;

➡Sezione di Riabilitazione Gastrenterologica Reumatologica e Vascolare, Via S. Maria Crocefissa di Rosa n.1, Valeggio sul Mincio (VR) con collegamento a 2 Mbps.

Art. 11 - Architettura di Sistema per l'Accesso alla Rete dell'Università degli Studi di Verona

L'accesso alla Rete di Ateneo ed ai Servizi sottoelencati è consentito all'interno di tutte le strutture dell'Ateneo solamente tramite credenziali GIA. Gli indirizzi IP pubblici e relativi parametri ad esso associati tutti i Client **DEVONO** essere assegnati dinamicamente dal Server DHCP di Ateneo e potrebbero variare ad ogni connessione.

L'infrastruttura di accesso alla rete di Ateneo distribuisce automaticamente i seguenti parametri di configurazione dell'indirizzo IP:

- indirizzo IP;
- maschera di sottorete;
- default gateway;
- server DNS;
- suffisso DNS;
- NTP server;

I dispositivi come stampanti, scanner, apparati di videosorveglianza, multifunzione, timbratrici etc...saranno collegati su apparati dedicati, e posizionati su VLAN appositamente predisposte, differenziate per tipologia di servizio, con indirizzamento IP privato

L’Area Reti provvede a conservare traccia dell’associazione tra utente e indirizzo dinamico assegnato per un periodo limitato ai fini di troubleshooting: contestualmente una copia dei log di accesso sono conservati per fini normativi sui log server di Ateneo. Il sistema consente un’elevata mobilità dell’utente, garantendo l’accesso in ogni struttura e garantendo la continuità della comunicazione al variare dei punti di accesso, sia wireless che cablati.

Art. 12 - Architettura di Sicurezza per Accessi dall’esterno

L’accesso alla rete di Ateneo dall’esterno è consentita **UNICAMENTE** tramite il Servizio SSLVPN. L’accesso SSLVPN è attualmente fruibile in due modalità: la prima via web autenticandosi con le proprie credenziali di accesso sul sito https://sslvpn.univr.it, la seconda in modalità client, mediante apposito software scaricabili dalla home page del servizio VPN in cui all’utente viene assegnato un indirizzo IP Pubblico.

Il Servizio VPN tiene traccia di ogni navigazione effettuata tramite autenticazione e logging in modo da poter risalire al mittente e responsabile della comunicazione ove necessario: anche in questo caso l’Area Reti provvede a conservare traccia degli accessi per un periodo limitato ai fini di troubleshooting: contestualmente una copia dei log di sono conservati per fini normativi sui log server di Ateneo

Art. 13 - I Servizi di Rete

I servizi disponibili sulla Rete di backbone dell'Ateneo sono quelli specifici della suite di protocolli Internet. Per sopravvenute esigenze di sicurezza o di necessità, alcuni servizi possono essere soppressi.

Una struttura può altresì erogare servizi informatici in rete compatibilmente con le politiche definite nel presente Regolamento, nelle Norme di Attuazione e in rispetto delle politiche GARR.

Per applicazioni che ad alto impatto (ad esempio videoconferenze, huge data transmission, …) di rete è necessaria l'autorizzazione esplicita del Dirigente dell'Area Informatica.

Le tipologie specifiche di Servizi di Rete sono le seguenti:

Servizio Firewall: L’Area Reti, per consentire agli utenti la massima disponibilità (fruibilità) del servizio di connettività, ha predisposto a tal fine apposite configurazioni e filtri a livello applicativo sui firewall, in modo da bloccare il transito di eventuali attacchi informatici o azioni ritenute pericolose e/o dannose, e prevedere anche condizioni di utilizzo a seconda della tipologia del servizio e/o dello status dell’utente.

Nessun pacchetto è ammesso in ingresso a condizione che non vi sia una corrispondente comunicazione in uscita oppure che non sia esplicitamente ammesso in quanto indirizzato a un Server;

I servizi, IP, TCP e UDP indirizzati a un Server devono essere esplicitamente richiesti e autorizzati;

La porta 25/TCP per il servizio smtp è aperta in uscita solo per i Server di posta autorizzati.
Sono ammesse deroghe alcune regole di filtro purché opportunamente documentate e approvate dal Dirigente Informatico o da persona da lui nominata. Le informazioni relative alle connessioni da e per Internet (tipo della connessione, mittente e destinatario) vengono registrate e conservate su apposito supporto per almeno 12 mesi, presso l'Area Sistemi.

Servizio Wireless: [Accesso tramite SSID UNIVAIR-WPA2 e UNIVAIR-OPEN]

La connessione alla rete wireless dell'Università degli Studi di Verona è gratuita.
L'utente che intende avvalersi del servizio Wireless deve attenersi al presente regolamento.

Il mancato rispetto del Regolamento comporterà immediati provvedimenti che saranno valutati a seconda della gravità dell'azione intrapresa e della sua recidività, fino alla disabilitazione permanente dei diritti di accesso.
L'utente che intende avvalersi del servizio wireless è tenuto a mantenere correttamente il proprio dispositivo conformemente a quanto stabilito all'Art. 2.

Servizio Autenticato di Accesso Rete Cablata (802.1x): E' un Servizio di autenticazione su rete cablata basato sullo standard IEEE 802.1x per controllare l'accesso alla rete tramite credenziali GIA.

Servizio SSL VPN (**S**ecure **S**ockets **L**ayer **V**irtual **P**rivate **N**etwork): La rete privata virtuale (VPN) fornisce un meccanismo di comunicazione protetta per i dati e le informazioni trasmesse. Il traffico delle informazioni che passano attraverso gli apparati ed il computer dell'utente finale è cifrato con il protocollo SSL o il suo successore, il Transport Layer Security (TLS).

Il servizio SSL VPN permette agli utenti istituzionali di realizzare una connessione da qualsiasi parte del mondo (Internet) verso la nostra rete di Ateneo (Intranet), attraverso un accesso via HTTPS (mediante una connessione cifrata quindi sicura) alle risorse informatiche e telematiche come se ci si trovasse all'interno della rete di Ateneo. Tale Servizio rappresenta la modalità più immediata e sicura, per raggiungere risorse bibliotecarie online tra cui Banche Dati e Riviste Full-Text.

Il servizio è gratuito ed esteso a tutti gli utenti dell'Ateneo (Personale, Docenti, Ricercatori, Studenti, Dottorandi, ecc…) utilizzando le proprie credenziali GIA.

Art. 14 - Regole di Utilizzo di Servizi di Rete con Accesso tramite le Federazioni EDUROAM/IDEM del Consorzio GARR

EDUROAM (EDUcation ROAMing): Con l'adesione dell'Ateneo di Verona alla Federazione Eduroam del Consorzio GARR gli utenti hanno la possibilità di usufruire gratuitamente di una connessione Internet wireless presso le sedi delle organizzazioni federate italiane e mondiali. L'Università di Verona offre questo Servizio Wireless per l'accesso ad Internet gratuitamente a tutti gli utenti interni con credenziali GIA e agli utenti esterni provenienti da istituzioni affiliate alla suddetta Federazione.

- ➡**SSID**: eduroam;
- ➡**Autenticazione**: WPA2 Enterprise;
- ➡**Cifratura**: WPA2 AES;
- ➡**Protocollo**: 802.1X;

➡**Credenziali**: Utente GIA esteso [codiceGIA**@ateneo.univr.it**].

IDEM (IDEntity Management per l'accesso federato): E' un servizio di autenticazione che permette agli utenti degli Enti Accademici e di Ricerca che hanno scelto di aderire alla federazione IDEM di utilizzare per l'accesso le proprie credenziali (quelle utilizzate nella propria istituzione) per accedere a risorse federate di tutte le istituzioni che partecipano al progetto.
L'Ateneo di Verona partecipa ad IDEM ed il servizio è fruibile gratuitamente da tutti gli Utenti dell'Ateneo con credenziali GIA.

Note sul rilascio degli attributi per l'uso dell'autenticazione federata IDEM-GARR-AAI per L'Università degli Studi di Verona.

Le credenziali per l'accesso ai servizi forniti dalla Federazione IDEM-GARR-AAI ed ai servizi interni offerti tramite il Service Provider dell'Università di Verona sono private e non cedibili ad alcuno per nessun motivo e a nessun titolo.

Il sistema di autenticazione rilascia al Service Provider esterno una serie di attributi LDAP indispensabili per l'autenticazione ed in assenza dei quali non è possibile la fornitura del servizio richiesto.
Tali attributi sono:
ou: Attributo descrittivo dell'Ateneo.
uid: Nome utente.
cn: Nome e cognome dell'utente.
givenName: Nome di battesimo dell'utente.
sn: Cognome dell'utente.
email: Indirizzo e-mail dell'utente.
telephoneNumber: Numero di telefono dell'utente. Il numero di telefono è richiesto esplicitamente da alcuni SP (per esempio Nilde).
preferredLanguage: Lingua preferita dall'utente (madrelingua).
eduPersonEntitlement: Abilitazioni particolari. L'entitling in particolare serve per poter accedere alle risorse bibliografiche
eduPersonPrincipalName: Attributo "scoped" derivato dall'uid. Gli attributi scoped derivano da quelli base con aggiunta del suffisso di organizzazione.
eduPersonAffiliation: Grado di affiliazione all'interno dell'organizzazione.
eduPersonScopedAffiliation: Scoped derivato dal precedente. Gli attributi scoped derivano da quelli base con aggiunta del suffisso di organizzazione.
eduPersonTargetedID: Attributo che permette la gestione di sessioni in forma anonima. Attributo che permette la gestione di sessioni in forma anonima calcolato grazie ad un algoritmo casuale e non riassegnabile.

Art. 15 - Posta Elettronica @univr.it

In conformità a quanto riportato all'Art. 4 del Regolamento tutti gli indirizzi, appartenenti al dominio univr.it in ragione della rilevanza esteriore attribuita all'indirizzo di posta elettronica, sono espressione dell'Università di Verona e della sua struttura organizzativa, pertanto è autorizzato un uso istituzionale. L'eventuale uso personale, comunque limitato, è soggetto alle disposizioni del presente Regolamento. Per garantire la natura istituzionale dell'indirizzo è compito di ciascun fruitore inserire in coda ad ogni messaggio spedito la seguente comunicazione anche in lingua

inglese: *Le informazioni trasmesse sono intese soltanto per la persona o l'ente cui sono indirizzate e possono avere contenuto confidenziale e/o riservato. La visione, la trasmissione, la diffusione o altro uso delle informazioni di cui sopra è proibita a chiunque ad esclusione del legittimo destinatario. Se avete ricevuto queste informazioni per errore, siete pregati di contattare il mittente e cancellare il materiale ricevuto.*
The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

L'Ateneo al fine di garantire l'attività ordinaria del servizio di posta elettronica, può trattare legittimamente in quanto necessario per la funzionalità del sistema, i dati delle caselle di posta elettronica nel rispetto delle norme, del diritto di riservatezza dell'utente e di terzi. Tali modalità sono disposte dal Dirigente della Direzione competente e di tale attività è redatta apposita annotazione.

L'Ateneo mette a disposizione di ciascun fruitore del servizio di posta elettronica apposite funzionalità di sistema, di agevole utilizzo, che consentono di inviare automaticamente, in caso di assenze (ad esempio per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É necessario avvalersi di tali modalità, prevenendo così l'eventuale ricorso da parte di terzi alla consultazione delle caselle di posta elettronica assegnate individualmente. In caso di eventuali assenze non programmate (ad esempio per malattia), qualora il lavoratore non possa attivare la procedura descritta il Responsabile del trattamento dei dati della struttura di appartenenza o afferenza del fruitore può disporre legittimamente, in casi di necessità ed urgenza, mediante personale appositamente incaricato (ad esempio gli amministratori dei sistemi, o della Direzione competente in materia oppure un fiduciario della persona assente, all'uopo da quest' ultima incaricata formalmente), l'attivazione di un analogo accorgimento. Di tale attività è redatto apposito verbale e informato l'interessato alla prima occasione utile.

Oltre a quanto regolamentato dal comma precedente, in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato può formalmente delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi e a inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. In assenza della nomina di un fiduciario, da effettuarsi entro tempi adeguati per l'espletamento della richiesta avanzata da parte del Titolare, con la presenza del Responsabile ai sensi della privacy del fruitore, di personale appositamente incaricato (ad esempio gli amministratori dei sistemi o della Direzione competente in materia) e di una rappresentanza sindacale dei lavoratori, il Titolare o persona da lui delegata, può legittimamente verificare il contenuto dei messaggi al fine da estrarre le informazioni ritenute rilevanti per lo svolgimento dell'attività lavorativa. A cura del Titolare del trattamento, di tale attività è redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile.

A richiesta del Responsabile della privacy delle strutture organizzative interessate, e' prevista l'attivazione di caselle istituzionali di posta elettronica condivise tra più lavoratori/fruitori. Le caselle istituzionali verranno condivise da membri delle strutture organizzative (unità / gruppo operativo, aree, direzioni, centri di responsabilità) della pianta organica di Ateneo oppure da incaricati allo svolgimenti di servizi interni o esterni gestiti dalle stesse. Per queste caselle

istituzionali verranno adottate regole di composizione degli indirizzi di posta elettronica, omogenee per tutto l'Ateneo, tali da identificare immediatamente le strutture organizzative o i servizi a cui sono assegnate.

Art. 16 - Gestione Server in Ateneo

É possibile attivare un Server per le diverse strutture dell'Ateneo, ospitati presso la Direzione Informatica o presso la struttura erogante i contenuti, tramite richiesta formale al Dirigente della Direzione Informatica da parte del Responsabile di Struttura.

La gestione del server e la responsabilità dei servizi erogati è del richiedente. I server di rete, per i quali sono previsto collegamenti Internet, devono essere autorizzati dal Dirigente della Direzione Informatica previa richiesta effettuata da uno strutturato e controfirmata dal Responsabile della struttura.

La richiesta deve essere indirizzata al Dirigente della Direzione Informatica indicando i parametri di funzionamento, la durata presunta di funzionamento del server e il nome dello strutturato richiedente che deve dichiarare di assumersi la responsabilità del funzionamento del Server. I

Il Dirigente della Direzione Informatica, nel valutare la richiesta, potrà fornire prescrizioni di natura tecnica e strutturale (es. potenziamento energia elettrica, sicurezza, …) che sono imprescindibili al fine dell'attivazione del server.

La richiesta deve contenere:

- ➡Le specifiche del sistema operativo e le metodologie con cui verranno effettuati sia gli aggiornamenti del sistema operativo che dell'eventuale software applicativo;
- ➡L'identificazione precisa dei servizi di rete che si intendono offrire, indicando le porte TCP e UDP di cui si richiede l'apertura verso Internet;
- ➡Il nome delle persone a cui è dato l'incarico di amministratore del sistema;
- ➡La configurazione dei meccanismi di logging, in particolare per gli accessi e i servizi, con un meccanismo di mantenimento delle informazioni di logging per un periodo di tempo previsto dalle attuali norme;
- ➡La protezione contro virus informatici e da accessi fisici incontrollati.

È comunque facoltà dell'Area Reti della Direzione Informatica chiedere l'immediata disconnessione dalla rete di qualunque Server qualora si venga a verificare una qualsiasi violazione del Regolamento o un grave evento di sicurezza che minacci la continuità operativa della rete di Ateneo.

Art. 17 - Titolarità del dominio DNS univr.it

Il dominio "univr.it" è assegnato all'Università degli Studi di Verona, è gestito dalla Direzione Informatica, che cura la gestione di tutti i domini di terzo livello[1] da esso dipendenti. L'Admin-C [2]per il dominio univr.it è il Direttore della Direzione Informatica.

I rapporti con la Naming Authority e con la Registration Authority italiane sono mantenuti dalla Direzione Informatica.

E' compito della Direzione Informatica di Ateneo mantenere un elenco, in forma elettronica, degli host registrati e rendere disponibili all'utenza i moduli relativi alle procedure di gestione del dominio.

Eventuali conflitti di nomi vengono risolti in accordo tra le parti. In caso di non accordo, i conflitti sono risolti di autorità dal Rettore, sentito il parere del Direttore della Direzione Informatica.

Art. 18 - Gestione dei domini di terzo livello interni ad univr.it

All'interno del dominio univr.it possono essere associati domini di terzo livello a Dipartimenti, Servizi, Istituti, Sezioni e Centri, oltre che ad Associazioni Culturali, Sindacali e Studentesche formalmente riconosciute ed operanti all'interno dell'Ateneo.

E' facoltà dei Dipartimenti richiedere l'attivazione e la registrazione di un proprio dominio di terzo livello composto dall'acronimo del nome del Dipartimento in italiano o dal nome del Dipartimento, anche abbreviato, che dovrà iniziare con la lettera "d": ad esempio Dipartimento di Informatica = di.univr.it .

Servizi, Istituti o Sezioni possono richiedere un proprio dominio di terzo livello composto dall'acronimo del nome del Servizio o Sezione in italiano, o da una abbreviazione del nome, che dovrà iniziare con la lettera "s": ad esempio Servizio di Farmacologia Medica = sfm.univr.it

I Centri possono avere un proprio dominio di terzo livello composto dall'acronimo del nome del Centro in italiano, o da una abbreviazione del nome che dovrà iniziare con la lettera "c", come ad esempio Centro Docimologico = cd.univr.it

Ogni Associazione formalmente riconosciuta dall'Ateneo può avere un proprio dominio di terzo livello, definito in modo che questo sia direttamente ed inequivocabilmente riconducibile alla denominazione dell'Associazione stessa.

Per l'attivazione e la registrazione dei domini in oggetto è sufficiente che il Responsabile della struttura o dell'associazione in oggetto richieda al Rettore l'attivazione e la registrazione dei server che si vogliono rendere noti all'esterno.

E' lasciata autonomia alla Direzione Informatica riguardo alla registrazione di nomi di terzo livello per server istituzionali (es. rs.univr.it per la Rassegna Stampa, ecc.) e per la creazione di domini di terzo livello funzionali all'organizzazione dei servizi informatici dell'Ateneo.

---

[1] Si definisce dominio di primo livello il suffisso posto a destra dell'ultimo punto all'interno di un nome di dominio (ad esempio "it" in .it, "net" in .net, ecc.). Si definisce dominio di secondo livello il nome posto a sinistra dell'ultimo punto (ad esempio "univr" in univr.it, "google" in google.it, ecc.). Si definisce dominio di terzo livello il nome posto a sinistra del penultimo punto all'interno di un nome di dominio (ad esempio "lettere" in lettere.univr.it). Analogamente, sono definiti i domini di quarto livello.

[2] Si definisce Admin-C il legale rappresentante che si assume la responsabilità del contenuto del dominio da registrare.

Art. 19 - Domini di secondo livello differenti da “univr.it”

Una Struttura interna all’Ateneo che richieda la registrazione di un dominio di secondo livello diverso da “univr.it” deve richiedere autorizzazione al Rettore.

Registrazioni di questo tipo sono possibili solamente in qualità di “alias” di una preesistente registrazione interna al dominio “univr.it”. In caso venga concesso questo tipo di registrazione, l’Admin-C per il dominio in oggetto è identificato in colui che effettua la richiesta al Rettore.

Nel caso si tratti di un dominio “.it”, la Lettera di Assunzione di Responsabilità deve essere firmata dal richiedente stesso, che si assume la piena responsabilità legale e civile nei confronti dei contenuti del dominio in oggetto e, per quanto concerne il server, anche a quanto determinato dalle leggi, dal Regolamento e dalle presenti Norme di attuazione.

Tutte le spese relative alla registrazione di un dominio di questo tipo sono a carico della Struttura richiedente.

La Direzione Informatica fornisce il supporto tecnico e organizzativo per la registrazione di domini di questo tipo.

Art. 20 - Domini di quarto livello. Modalità di richiesta e durata delle registrazioni

È facoltà delle Strutture la completa autonomia nel richiedere e gestire nomi a dominio di quarto livello, purché in conformità con quanto disposto dal presente articolo.

Possono essere assegnati nomi di quarto livello solamente agli individui. Tale assegnazione non è consentita ai fruitori delle biblioteche ed agli Studenti dei Corsi di Laurea e Master, fatti salvi i Responsabili di Associazioni Studentesche ufficialmente identificati.

La richiesta di registrazione di nomi di quarto livello all’interno dei domini di terzo livello va effettuata mediante apposito modulo in cui dovranno essere indicati:

- la Struttura di riferimento (e quindi il dominio di terzo livello)
- il Richiedente la registrazione, che diventerà il Responsabile presso l’Ateneo dei contenuti del server, che si assume la piena responsabilità legale e civile nei confronti dei contenuti del dominio in oggetto e, per quanto concerne il server, , dovranno essere mantenuti costantemente in adeguate condizioni di sicurezza ed essere conformi a quanto disposto dalle necessarie e previste funzioni di privacy, accesso e monitoraggio di cui alle norme e regolamenti in vigore.
- l’indirizzo di rete corrispondente alla registrazione richiesta
- una breve descrizione dei servizi erogati del dispositivo che si intende registrare
- l’eventuale necessità di rendere il dispositivo raggiungibile dall’esterno della rete di Ateneo (in caso contrario sarà identificabile solamente dalle postazioni interne alla rete di Ateneo)
- l’eventuale presenza di una denominazione pregressa, nel cui caso si richiede la registrazione di un alias.
- un indirizzo di posta elettronica istituzionale e un numero di telefono interno del Richiedente

Il modulo di richiesta dovrà recare timbro e firma del Responsabile della Struttura cui appartiene il Richiedente e la firma del Richiedente stesso, ed essere inoltrato alla Direzione Informatica.

In caso di cessazione del rapporto tra il Richiedente e l'Ateneo, la responsabilità dei contenuti del server ricade sul Responsabile della Struttura a cui il server fa riferimento, o su chi ne occupi la medesima posizione nei confronti dell'Ateneo.

Ogni registrazione, escluse quelle relative ai domini di terzo livello che fanno riferimento a Strutture interne all'Ateneo e quelle effettuate dalla Direzione Informatica, avrà una durata di due anni.
Al termine del periodo di validità della registrazione, il Richiedente (o, in sua assenza, il Responsabile della Struttura), verranno contattati dalla Direzione Informatica per il rinnovo della registrazione. In caso di risposta negativa o di mancata risposta, la registrazione verrà cancellata in un periodo compreso tra i 30 ed i 60gg.
Il ripristino di una registrazione cancellata seguirà la stessa procedura di una nuova registrazione.

Art. 21 - Portale di Ateneo e Siti Web

Il sito ufficiale Web dell'Ateneo è www.univr.it e viene gestito dall'Area Sviluppo e Web della Direzione Informatica.

L'Area Sviluppo e Web ha il compito di predisporre i siti Web "istituzionali" per le strutture che ne facciano richiesta. Sono definiti "istituzionali" i siti Web strettamente collegati alla didattica (Dipartimenti e Scuole) e alla ricerca (Dipartimenti e Centri) svolti nell'Università e quelli appartenenti all'area amministrativa e ai Servizi dell'Ateneo.

Per ogni sito istituzionale si definiscono due figure, il responsabile e il referente. Il responsabile del sito Web è il responsabile della struttura stessa ed è anche responsabile dei contenuti inseriti nel sito Web di sua pertinenza all'interno del Portale d'Ateneo. Il responsabile di un sito Web può decidere di indicare un referente Web con un compito più tecnico e che dovrà mantenere i necessari contatti con la Direzione Informatica. In caso di mancata nomina il responsabile del sito è anche considerato il suo referente.

Tutti i siti istituzionali devono uniformarsi alle scelte tecnologiche operate dalla Direzione Informatica. Inoltre, L'Area Sviluppo e Web si limita alla sola predisposizione del sito, in quanto l'inserimento e l'aggiornamento dei contenuti sono delegati ai responsabili/referenti.

I Server Web non devono costituire potenziale fonte di rischio informatico o compromettere l'immagine dell'Ateneo e rispettare la "Acceptable Use Policy della rete GARR" e il Regolamento. L'Area Reti della Direzione Informatica è il referente tecnico per il portale d'Ateneo e per tutti i siti che abbiano un qualunque indirizzo nel dominio univr.it.

Art. 22 - Rilevazione e Gestione degli Incidenti per la Sicurezza

É compito dell'Area preposta alla gestione di un Servizio erogato predisporre meccanismi tecnici e organizzativi per il monitoraggio periodico, anche quotidiano. In caso di rilevazione di incidente, il Dirigente della Direzione Informatica o l'Area della Direzione Informatica coinvolta informerà tutti gli interessati in modo tempestivo.

Si dovrà altresì provvedere nel più breve tempo possibile al ripristino del servizio compatibilmente con l'eventuale necessità di individuare prioritariamente la causa dell'incidente interrompendo temporaneamente il servizio stesso. Si dovrà inoltre ripristinare il Servizio avendo cura di mantenere adeguatamente le informazioni utili per la descrizione dell'incidente.

I principi fondamentali di sicurezza dei servizi erogati sulla rete dell'Ateneo sono descritti nelle Norme di Attuazione, mentre le misure di sicurezza puntuali messe in opera sono elencate nel Documento Programmatico sulla Sicurezza redatto/aggiornato a cura degli uffici preposti e approvato dal Consiglio di Amministrazione.

Art. 23 - Monitoraggio e Controllo

I dati di traffico sono conservati e suscettibili di accesso conformemente a quanto disposto dalle norme vigenti in materia di Privacy.

In presenza di situazioni dannose o di pericolo per le funzionalità della rete di Ateneo segnalate da strumentazioni, controlli da parte degli operatori o da enti esterni legittimamente preposti, il Dirigente della Direzione competente o il l'Area Reti della Direzione Informatica possono adottare misure immediate che consentano il superamento delle citate situazioni.

In caso di segnalazione, possono essere disposti da parte del Titolare o. nei casi di urgenza, dal Dirigente della Direzione competete, tramite strumentazioni automatiche o azioni manuali, controlli sull'utilizzo delle risorse posta elettronica, intranet e Internet.

Nell'adottare le predette misure e nell'effettuare controlli sull'uso degli strumenti elettronici è comunque garantito il rispetto del principio di necessità e di minimizzazione dell'utilizzo dei dati dell'interessato, evitando l'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei fruitori, come pure su eventuali soggetti esterni che ricevano o inviino comunicazioni elettroniche di natura personale o privata.

In caso di abusi singoli o reiterati vengono di norma inoltrati, a cura del Titolare, preventivi avvisi collettivi o individuali e disposti controlli nominativi o su singoli dispositivi e postazioni. L'avviso può riguardare il rilevato utilizzo anomalo degli strumenti aziendali e contenere l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite.

Art. 24 - Memorizzazione dei File di Log

In conformità a quanto riportato dall'Art. 6 del Regolamento, i sistemi che memorizzano i file di Log sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra registrazione come, ad esempio, la cosiddetta "rotazione dei log file") i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia imposta da vigenti norme, regolamenti o policy.

Per quanto riguarda il trattamento dei dati di Log:

- ➡I dati di Log raccolti, dopo un periodo di trenta giorni, sono conservati in forma crittografata. Le chiavi di crittografia sono mantenute dal Titolare e dal Dirigente della Direzione competente;

➡La conservazione di dati di Log, sia crittografati che non, avviene per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive, di sicurezza e di controllo e per quanto dispone la normativa in materia;

➡Per quanto concerne i dati di log raccolti e non ancora memorizzati in modalità crittografata, il trattamento viene effettuato dal Dirigente della Direzione competente, dal personale dell'Area che sovraintende le reti e dell'Area che sovraintende i sistemi della Direzione competente che, in forza del presente Regolamento, sono da considerarsi incaricati a trattare i dati di log nelle modalità strettamente necessarie nell'ambito dell'espletamento delle azioni ordinarie e quotidiane di mantenimento della rete e delle risorse, oltre che nell'ambito del trattamento previsto dal loro status individuale di amministratore di sistema;

➡Ogni trattamento riferibile a dati di log già memorizzati in forma crittografata deve avvenire solamente a seguito di istanza presentata dagli organi competenti di pubblica sicurezza o dal Titolare;