CITTÀ METROPOLITANA DI BOLOGNA

DISCIPLINARE INTERNO PER L'ACCESSO E L'UTILIZZO DEI SERVIZI INFORMATICI DELLA CITTÀ METROPOLITANA DI BOLOGNA

Sommario

Il presente disciplinare, adottato sulla base e secondo le indicazioni contenute nella circolare AGID del 18/04/2017 (disposizioni in materia di sicurezza informatica), nel Regolamento UE 2016/679 del 27/04/2016 (GDPR - regolamento generale sulla protezione dei dati) e nella direttiva della Presidenza Consiglio Ministri n. 02/09 (utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro), ha per oggetto i criteri e le modalità di utilizzo del servizio di posta elettronica ed internet e, più in generale, delle dotazioni informatiche della Città metropolitana di Bologna da parte dei propri dipendenti e dei collaboratori atipici che, a vario titolo, svolgono un'attività per conto della Città metropolitana di Bologna accedendo al suddetto sistema informatico (di seguito, "utenti").

1. Finalità

Il presente Disciplinare ha lo scopo di:

- porre in essere ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri degli strumenti informatici, della Rete Informatica e Telematica e del Sistema di telefonia fissa e mobile, nel rispetto dei diritti dei lavoratori e del diritto alla riservatezza;
- garantire il diritto alla riservatezza degli utenti interni ed esterni della Rete Informatica, Telematica e di Telefonia;
- assicurare la funzionalità ed il corretto impiego delle strumentazioni informatiche e telematiche da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa;
- prevenire rischi alla sicurezza del sistema;
- responsabilizzare gli utilizzatori sulle conseguenze di un uso improprio delle strumentazioni;
- definire in maniera trasparente le modalità di effettuazione dei controlli e le conseguenze, anche disciplinari, di un utilizzo indebito.

2. Modalità di accesso alla rete ed utilizzo delle postazioni informatiche

Per accedere ai servizi informatici da una postazione di lavoro l'utente deve utilizzare un codice identificativo (id utente) e una parola chiave segreta (password).

Superato il sistema di autenticazione, l'utente è collegato alla rete della Città metropolitana di Bologna e ad internet.

Ciascuna postazione di lavoro è assegnata nominalmente ad un utente dall' U.o. Sviluppo e Gestione Sistemi. In caso di necessità operativa è sempre possibile, da parte di ciascun utente, accedere alla rete tramite un'altra postazione utilizzando le proprie credenziali.

L'utente deve essere consapevole del fatto che permettere l'accesso a terzi con le proprie credenziali lo espone a responsabilità civile e penale per eventuali utilizzi illeciti.

Preso atto di tale conseguenza, l'utente si impegna a:

- mantenere riservata la password;
- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione ad altri;
- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali; nel caso l'utente abbia necessità di allontanarsi deve bloccare la propria stazione di lavoro utilizzando la sequenza di tasti 'ctrl-alt-canc' e il tasto 'blocca'. E' evidente

che lasciare un PC incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso;

- non utilizzare le postazioni lasciate incustodite e sbloccate dai colleghi.

Le attività di gestione e manutenzione dei Personal Computer dell'Ente fanno capo all' U.o. Sviluppo e Gestione Sistemi e non è permesso agli utenti di intervenire personalmente sulle apparecchiature informatiche.

In particolare:

- è proibito installare programmi software non autorizzati, anche se legali, e/o modificare la configurazione hardware della propria postazione di lavoro. Qualora venissero trovati programmi non autorizzati sulle stazioni di lavoro questi verranno disinstallati dal personale tecnico addetto alla manutenzione dei Personal Computer
- l'Ente mette a disposizione degli utenti differenti sistemi di memorizzazione su cui effettuare il salvataggio e la condivisione dei documenti e dei files di lavoro: i dischi di rete, identificati sulle Pdl da lettere (F:, R:, etc) ed il sistema in cloud 'Owncloud', utilizzabile attraverso un browser Web. Su queste unità vengono svolte attività di amministrazione e salvataggio periodico (backup). Questi sistemi non possono essere utilizzati per il salvataggio di file privati o comunque non inerenti all'attività lavorativa. Il personale tecnico dell'U.o. Sviluppo e Gestione Sistemi potrà procedere alla rimozione di files o applicazioni ritenute pericolosi per la sicurezza del sistema o non relativi all'attività d'ufficio
- tutti i documenti relativi all'attività lavorativa devono essere salvati sui sistemi di memorizzazione in rete definiti al punto precedente, in aree private o condivise. I files salvati su differenti unità di memorizzazione (dischi interni alle Pdl, chiavette USB, etc..) non sono recuperabili in caso di guasto dell'unità di memorizzazione e non saranno salvati e/o ricopiati in caso di sostituzione della Pdl
- nell'utilizzo di programmi, materiali audiovisivi, documenti ed ogni altra informazione digitale protetta a norma di legge gli utenti devono rispettare diritti d'autore, copyright e licenze d'uso di software
- non è permesso l'utilizzo e/o la connessione alla propria Pdl o in rete di sistemi o periferiche hardware private non autorizzate dal personale tecnico dell' U.o. Sviluppo e Gestione Sistemi
- è vietato pubblicare o diffondere, anche tramite social network, notizie e informazioni di cui il dipendente sia venuto a conoscenza per ragione di ufficio. Ugualmente, si astiene dal

pubblicare, su siti leggibili da più utenti, nel rispetto della libertà del diritto di corrispondenza, dichiarazioni offensive nei confronti dell'Amministrazione, dei colleghi e dei collaboratori.

3. Modalità di utilizzo della strumentazione informatica dell'Ente in Smart Working/ Lavoro Agile

Al fine di rendere possibile lo svolgimento della prestazione lavorativa il dipendente, potrà essere dotato dall'Amministrazione di un personal computer portatile ed eventualmente di un cellulare, da utilizzarsi nel totale rispetto delle regole determinate dalla regolamentazione e in conformità con le indicazioni che gli saranno fornite.

Gli strumenti di lavoro affidati al dipendente devono essere usati esclusivamente per lo svolgimento dell'attività lavorativa, nel rispetto di quanto previsto dai regolamenti dell'Amministrazione, e non per scopi personali o non connessi all'attività lavorativa.

Il dipendente ha l'obbligo di utilizzare e custodire gli strumenti di lavoro affidatigli con la massima cura e diligenza; un utilizzo scorretto degli strumenti messi a disposizione costituisce motivo di inadempimento di valenza disciplinare.

In caso di guasto delle attrezzature in dotazione il lavoratore dovrà dare immediato avviso al proprio responsabile, all'assistenza informatica e dovrà consegnare lo strumento guastato non appena possibile.

Il dipendente che effettua attività di smart-working può collegare il portatile messo a disposizione dall'Ente alla propria rete WI-FI per finalità istituzionali connesse alle attività lavorative svolte e nel rispetto del presente Disciplinare.

Per l'accesso alla rete dell'Ente viene utilizzato un programma installato sul portatile (VPN), che garantendo un accesso sicuro ai sistemi informatici dell'Ente, permette all'utente di svolgere l'attività lavorativa in modalità analoga a quella dell'ufficio.

Indipendentemente dalla modalità di lavoro, l'utente deve effettuare periodicamente connessioni attraverso la VPN per permettere l'installazione di aggiornamenti del sistema, di programmi e lo scarico delle politiche di sicurezza.

L'utente potrà utilizzare, nel caso in cui non possa disporre di strumentazione fornita dall'Ente, apparecchiature di proprietà per svolgere attività lavorativa in smartworking.

L'uso di strumentazione propria dovrà essere autorizzato dal personale tecnico dell'U.o. Sviluppo e Gestione Sistemi, che ne valuterà la compatibilità con i sistemi utilizzati dall'Ente e verificherà che dispongano dei requisiti di sicurezza necessari.

In questo caso verrà richiesto all'utente, che confermerà di svolgere l'attività con una autodichiarazione, di installare alcuni programmi necessari per accedere ai servizi informatici e di mantenere i sistemi e l'antivirus aggiornati.

Nel caso di utilizzo di sistemi di proprietà verrà fornita assistenza solo sulle componenti software che saranno fornite dall'Ente.

In particolare si richiama la necessità di verificare che l'antivirus installato sul computer sia attivo, aggiornato e connesso al server di gestione.

Nel caso in cui ci sia necessità di connettersi a rete wireless diverse da quella della propria abitazione si raccomanda, al fine di prevenire l'esposizione a cyber attacchi, di evitare il collegamento a reti non sicure o sulle quali non si siano presenti adeguati sistemi di protezione e sicurezza.

4. Posta Elettronica

Il servizio di posta elettronica è disponibile per ogni dipendente in forma centralizzata.

L'indirizzo di posta elettronica è composto da nome.cognome@cittametropolitana.bo.it (in caso di omonimia viene aggiunto un numero sequenziale).

Sono inoltre messe a disposizione degli uffici indirizzi di posta elettronica non nominali, condivisi fra più utenti, che possono essere richiesti da Dirigenti e p.o. utilizzando un modulo a disposizione sulla intranet.

Nell'utilizzo della posta devono essere adottate le seguenti misure di tipo organizzativo-tecnologico:

- l'assegnazione della casella di posta avviene unicamente per ragioni di servizio;
- le caselle nominali sono da ritenersi personali e accessibili esclusivamente da parte dell'utente proprietario attraverso l'inserimento di una password; la password deve essere mantenuta riservata e non deve essere comunicata. L'utente, utilizzando le apposite funzioni di delega fornite dal sistema di posta può comunque concedere, in caso di necessità e per ragioni di servizio, l'accesso e l'utilizzo della propria casella ad altri colleghi. I diritti di utilizzo delle caselle di posta non nominali sono stabiliti dall' U.o. Sviluppo e Gestione Sistemi su richiesta di Dirigenti o p.o. ;
- per evitare di far inserire il dominio @cittametropolitana.bo.it in blacklist di gestori di posta esterni, bloccando di fatto tutte le mail in uscita dell'ente, si è posto a 500 il limite massimo di mail inviabili in un'ora a indirizzi di posta esterni all'ente;
- l'invio di e-mail con allegati a mittenti multipli deve essere limitata onde evitare sovraccarico

sul server centrale e sulle linee esterne. La dimensione massima degli allegati accettati dal sistema di posta è 15 Megabytes;

- è a disposizione di ciascun lavoratore una apposita funzionalità di sistema che consente di inviare automaticamente, in caso di assenze programmate, messaggi di risposta personalizzabili segnalando eventualmente l'indirizzo della persona da contattare;
- È buona norma limitare la lunghezza del messaggio. Specie se si risponde (reply) ad un messaggio, riportando il contenuto del messaggio originale, conviene lasciare solo quelle parti che sono rilevanti per la risposta;
- le caselle di posta elettronica devono essere utilizzate cancellando sistematicamente i messaggi non necessari per ragioni di servizio, quelli con allegati ingombranti che vanno scaricati negli appositi dischi, quelli a contenuto pubblicitario e spam.
- è doveroso informare tempestivamente l'Ente e l'Amministratore di sistema su potenziali rischi o problemi inerenti alla sicurezza informatica della posta elettronica.
- verificare il destinatario del messaggio prima dell'invio e non utilizzare la modalità 'rispondi a tutti' se non realmente necessaria.

In ogni caso è tassativamente vietato:

- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di
- distribuzione esterne o di azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare 'catene di S. Antonio', appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), giochi, scherzi, barzellette, messaggi inerenti a virus, etc…;
- utilizzare la casella personale per l'iscrizione a dibattiti, forum o mailing-list se non inerenti alla propria attività lavorativa;
- utilizzare il servizio di posta elettronica per trasmettere pubblicità personale o commerciale.

5. Utilizzo del sistema cloud "MetroCloud" per la condivisione di documenti

Metrocloud è un sistema, basato su cloud privato, che permette la condivisione di documenti e files non solo fra gli utenti interni ma anche con utenti esterni all'Ente.

Nel caso risulti necessario, per esigenze aziendali, condividere documenti di lavoro, anche di grosse dimensioni, con persone esterne all'Ente, è possibile utilizzare questo sistema raggiungibile tramite l'indirizzo https://metrocloud.cittametropolitana.bo.it.

Tale sistema può essere quindi utilizzato anche come deposito temporaneo per lo scambio di files.

In questo caso i documenti devono permanere per il tempo necessario per il recupero da parte della persona destinataria. L'accesso ai documenti deve essere sempre consentito mediante password.

Il sistema MetroCloud permette l'accesso ai files da Internet utilizzando le proprie credenziali di lavoro, anche utilizzando 'app' per device di tipo mobile.

Il dipendente nell'utilizzo della documentazione messa a sua disposizione dall'Amministrazione tramite il sistema MetroCloud dovrà rispettare le disposizioni eventualmente accordate e potrà utilizzare i documenti stessi per le sole finalità espressamente riconosciute all'atto della condivisione del materiale.

In questo ambiente i diritti di accesso ai documenti memorizzati vengono direttamente gestiti dagli utenti, che quindi possono definire chi può avere accesso al singolo documento o cartella e in quale modalità.

Essendo un sistema connesso ad internet la cui protezione è basata sulla password si raccomanda:

- di mantenere la password riservata e non concedere a nessuno l'accesso ai sistemi tramite le proprie credenziali
- di verificare con attenzione con chi si condivide l'accesso ai documenti e di concedere i diritti minimi necessari a svolgere l'attività richiesta (per esempio: se un documento non deve essere modificato da altri concedere solo accesso in lettura)
- di dare accesso ai documenti ad esterni sempre mediante password e preferibilmente definire una data di scadenza della validità della condivisione

Si rimanda al paragrafo 1 per ulteriori specifiche sull'uso della condivisione dei files.

6. Utilizzo sistemi di videoconferenza

I sistemi di videoconferenza utilizzati all'interno dell'Ente sono:

- Lifesize: per organizzare sistemi di videoconferenza con un ampio numero di partecipanti. Sono a disposizione degli utenti 'stanze' virtuali permanenti che possono essere prenotate dall' agenda della posta Zimbra al momento di convocazione di una riunione. Altre stanze temporanee possono essere create dai gestori del sistema. Le riunioni devono essere organizzate preventivamente in quanto i partecipanti devono conoscere il link al quale connettersi.
- Teams: è una componente di videoconferenza all'interno della posta Zimbra e permette di

effettuare riunioni con un numero limitato di partecipanti. Ogni utente ha a disposizione una propria stanza virtuale o può crearne ulteriori se necessario.

Si ricorda:

- che i sistemi di videoconferenza sono strumenti di lavoro da utilizzare in alternativa a riunioni in presenza o come alternativa alla chiamata telefonica
- di dotarsi di cuffie con microfono (per esempio anche quelle del telefono cellulare) . Questo migliora sensibilmente la qualità del segnale audio.
- di spegnere il proprio microfono quando non utilizzato per evitare di introdurre rumori, brusii o interferenze.
- che nel caso ci si connetta dalla propria abitazione e non si disponga di una zona riservata è possibile utilizzare sfondi (disponibili su Lifesize) virtuali, o, se si preferisce, disattivare la videocamera.
- che nel caso in cui non si disponga di banda sufficiente a garantire un adeguato segnale audio- video è conveniente spegnere la videocamera
- di scollegarsi sempre al termine della videoconferenza, La stessa stanza potrebbe essere utilizzata successivamente per altre riunioni.

7. Utilizzo di Internet

Tutti gli utenti in possesso di credenziali per accedere alla rete interna dell'Ente possono collegarsi alla rete internet il cui utilizzo è consentito unicamente per ragioni di servizio.
L'utente è direttamente responsabile dell'uso di internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.
L'utilizzo imprudente di alcuni servizi della rete Internet può essere fonte di particolari minacce alla sicurezza del sistema (esempio virus informatici) e all'immagine dell'Ente.

Nell'utilizzo di internet è vietato:

- lo scarico (upload e/o download) di files e/o programmi software, se non esplicitamente autorizzati;
- la partecipazione a Forum non autorizzati, l'utilizzo di chat line, di bacheche elettroniche e la registrazione in guestbooks anche utilizzando pseudonimi (o nicknames) e, più in generale, qualunque utilizzo di questi servizi Internet se non strettamente connessi all'attività lavorativa;

- l'utilizzo del collegamento ad internet per attività in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- l'utilizzo di sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting o similari, così come connettersi a siti che trasmettono programmi in streaming (come radio o TV via WEB) senza espressa autorizzazione.

Tuttavia l'utilizzo di internet per svolgere attività che non rientrano tra i compiti istituzionali può essere consentito ai dipendenti per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro purchè contenuta nei tempi strettamente necessari allo svolgimento di tali transazioni (ad esempio, per effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e assicurativi).

8. Monitoraggio e controlli

L'Ente ha predisposto il proprio sistema informativo e la rete intranet ed internet per esclusive esigenze organizzative e/o produttive. A tal fine si avvale legittimamente di sistemi che consentono indirettamente un controllo di eventi potenzialmente pericolosi sulla rete.

Non saranno utilizzati sistemi hardware e/o software idonei ad effettuare un controllo a distanza dei lavoratori, in particolare mediante:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore; • la lettura o la registrazione dei caratteri inseriti tramite la tastiera e analogo dispositivo.

Sono comunque esclusi controlli prolungati, costanti e/o indiscriminati.
Le attività sull'uso del servizio di accesso ad internet e all'accesso ai servizi informatici vengano automaticamente registrate in forma elettronica attraverso i LOG di sistema.
Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.
I dati personali contenuti nei LOG possono essere trattati in via eccezionale e tassativamente nelle

seguenti ipotesi:

- per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
- quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
- ove richiesti dal Direttore Generale a seguito di segnalazione scritta e motivata da parte di un dirigente che abbia ravvisato o presuma, sulla base di gravi indizi, comportamenti di un dipendente o collaboratore ad esso assegnati, in qualsiasi modo non conformi a quanto previsto dal presente disciplinare.

I dati contenuti nei LOG sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a una settimana lavorativa, e sono periodicamente cancellati automaticamente dal sistema.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e avverrà solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria e della polizia giudiziaria.

In questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità esplicitati.

I dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell'utente che ha effettuato l'installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

9. Interruzione e cessazione del servizio

Eventuali interruzioni del servizio sono comunicate agli utenti.

L'utilizzo del servizio di accesso alla rete ed al sistema informatico dell'Ente viene disabilitato quando, per una qualunque ragione, viene interrotto il rapporto lavorativo con la Città metropolitana di Bologna, il giorno successivo a quello della scadenza del contratto.

10. Responsabilità e sanzioni

L'utente delle risorse informatiche della Città metropolitana di Bologna che abbia violato il presente disciplinare o la normativa ivi richiamata, potrà essere soggetto ad azione disciplinare in conformità a quanto stabilito dai contratti collettivi e dagli artt. 54 e seguenti del D.lgs. n. 165/2001 nonchè dal Codice disciplinare e di comportamento della Città metropolitana di Bologna, fatta salva la possibilità

per l'Ente di esercitare le opportune azioni giudiziarie nelle sedi competenti, a tutela dei propri diritti giuridicamente tutelati.

In caso di danno, la violazione espone altresì l'utente responsabile ad azioni legali di carattere civile o penale da parte dei danneggiati e a richieste di risarcimento anche da parte della Città metropolitana di Bologna.

11. Glossario

Backup: il termine, che significa copia di sicurezza, indica l'operazione di duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server. Normalmente viene svolta con una periodicità stabilita.

Chat: (letteralmente, "chiacchierata") è un servizio informatico che permette attraverso internet, di attivare e gestire un dialogo in tempo reale fra due o più utenti utilizzando principalmente messaggi testuali.

File sharing: condivisione di file all'interno di una rete comune.

Forum: generalmente si riferisce ad un archivio informatico contenente discussioni e messaggi scritti dagli utenti oppure al software utilizzato per fornire questo archivio. Ci si riferisce comunemente ai forum anche come board, message board, bulletin board, gruppi di discussione, bacheche e simili.

Guestbook: (letteralmente, libro degli ospiti) è un servizio interattivo che permette ai visitatori di un sito web di poter lasciare 'firme' e commenti.

ID utente: codice identificativo personale per l'accesso ai sistemi informatici. Normalmente è formato dal cognome o dal cognome e parte del nome.

LOG: il termine, che significa giornale di bordo o semplicemente giornale, viene utilizzato nell'informatica per indicare la registrazione cronologica delle operazioni man mano che vengono eseguite ed il file su cui tali registrazioni sono memorizzate.

Mailing-list: (letteralmente, lista per corrispondenza traducibile in italiano con lista di diffusione) è un sistema organizzato per la partecipazione di più persone in una discussione tramite posta

elettronica.

Mail spamming: è l'invio di grandi quantità di messaggi indesiderati (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è internet attraverso l'e-mail.

Password: (in italiano: “parola chiave”, “parola d'ordine”, o anche “parola d'accesso”) è una sequenza di caratteri utilizzata per accedere ad una risorsa informatica.

Podcasting: sistema che permette di scaricare in modo automatico documenti (generalmente audio o video) chiamati podcast, utilizzando un programma generalmente gratuito chiamato aggregatore o feeder. Con podcast si intende un file (generalmente audio o video), messo a disposizione su Internet e scaricabile automaticamente.

Software freeware: programmi software distribuiti in modo gratuito.

Software peer-to-peer: programmi utilizzati per la condivisione e lo scambio di files fra elaboratori. Questi programmi vengono utilizzati principalmente per scambiarsi file di tipo mp3, (file musicali) e DivX (contenenti i film) spesso in violazione dei diritti d'autore.

Stand - alone: si riferisce ad un’apparecchiatura capace di funzionare da sola, indipendentemente dalla presenza di altre apparecchiature con cui potrebbe comunque interagire.

Streaming: identifica un flusso di dati audio/video trasmessi da una sorgente a una o più destinazioni tramite una rete telematica. Questi dati vengono riprodotti man mano che arrivano a destinazione.

Webcast/Webcasting: descrive la trasmissione di segnale audio o video, in tempo reale o ritardato, mediante tecnologie web. Il suono o il video sono catturati con sistemi audio-video convenzionali, quindi digitalizzati e inviati in streaming su un web server. Un client webcast consente agli utenti di connettersi ad un server che sta distribuendo (operazione detta di webcasting) e di ascoltare o visualizzare il contenuto audio/video.

.