Università degli Studi di Salerno
Corso di Ingegneria del Software

FakeNews Checker
Problem Statement
Versione 1.1

Data: 14/10/2025

Coordinatore del progetto:

Nome	Matricola
Swami Falasca	0512119323

Partecipanti:

Nome	Matricola
Federica De Simone	0512120472
Giuseppe Tirelli	0512120367
Swami Falasca	0512119323

Scritto da:	Swami Falasca, Federica De Simone, Giuseppe Tirelli

Revision History

Data	Versione	Descrizione	Autore
13/10/2025	1.0	Prima versione del Problem Statement	Swami Falasca, Federica De Simone, Giuseppe Tirelli
14/10/2025	1.1	Nuova versione Problem Statement	Federica De Simone, Swami Falasca, Giuseppe Tirelli

INDICE

1. PROBLEM STATEMENT

PURPOSE

Lo scopo di questo documento è stabilire una comprensione condivisa tra il team di progetto e il cliente in merito al problema affrontato dal sistema FakeNews Checker. Nell'era digitale, la disinformazione si diffonde rapidamente attraverso i canali online, plasmando l'opinione pubblica e spesso portando a incomprensioni o manipolazioni.
FakeNews Checker mira a contrastare questo fenomeno fornendo una piattaforma web accessibile che consente agli utenti di leggere notizie, segnalare articoli sospetti e confrontarli con fonti verificate e affidabili.
Questo documento descrive il contesto attuale del problema, delinea le funzionalità richieste, specifica l'ambiente operativo e definisce i risultati del progetto, le scadenze e i criteri di accettazione.

AUDIENCE

FakeNews Checker è destinato a:

- Il *cliente*: l'organizzazione che richiede lo sviluppo della piattaforma anti-disinformazione.
- Gli *utenti finali*:
  - Utente non registrato: consulta le notizie pubblicate
  - Utente registrato: consulta le notizie, segnala contenuti sospetti, invia articoli per la verifica e gestisce il profilo
- Gli *amministratori di sistema*:
  - Amministratore Tecnico: gestisce la piattaforma a livello tecnico
  - Amministratore delle Verifiche: esamina le segnalazioni e approva o rimuove notizie

1.1 PROBLEM DOMAIN

L'ascesa dei media digitali e delle piattaforme social ha aumentato drasticamente la velocità e la portata della diffusione delle informazioni. Sfortunatamente, questo ha anche facilitato la diffusione di fake news, contenuti falsi o fuorvianti progettati per manipolare l'opinione pubblica o generare profitto attraverso il coinvolgimento. Molti utenti non hanno gli strumenti o le conoscenze per verificare se una notizia è attendibile. L'assenza di sistemi centralizzati e di facile utilizzo per la verifica delle informazioni online contribuisce alla diffusione della disinformazione e alla confusione pubblica.

1.1.1 OBIETTIVI

Gli obiettivi della piattaforma sono:

- Fornire agli utenti una fonte affidabile di notizie verificate,
- Consentire la segnalazione e la verifica di contenuti sospetti,
- Promuovere la consapevolezza digitale e il pensiero critico tra i lettori.

2. SCENARIOS

2.1 UTENTE NON REGISTRATO

2.1.1 Consultazione delle notizie

Marta è una studentessa interessata all'attualità e, dopo aver sentito parlare del portale **FakeNews Checker**, decide di visitarlo per tenersi informata su notizie verificate.
Accedendo alla homepage tramite il browser del suo computer, il sistema le mostra una lista di articoli corredati da titolo, descrizione, immagine e un indicatore che segnala lo stato della notizia: *"Verificata"*, *"In verifica"* oppure *"Non attendibile"*.

Marta scorre l'elenco e clicca su un articolo che attira la sua attenzione. La piattaforma apre la pagina dedicata, dove può leggere l'intero testo, consultare la fonte originale tramite link e visualizzare eventuali informazioni sull'autore e la data di pubblicazione.

Durante la lettura, nota la presenza di un pulsante **"Segnala come sospetta"**, che però risulta disattivato in quanto riservato solo agli utenti registrati.
Terminata la lettura, Marta decide di utilizzare la barra di ricerca per cercare altri articoli.

Dopo aver navigato per un po', si rende conto che vorrebbe partecipare al progetto, magari segnalando notizie sospette o inviando nuovi articoli. Per farlo, clicca su **"Registrati / Accedi"**, venendo indirizzata alla pagina di registrazione.

Il sistema la invita a inserire il proprio indirizzo e-mail e una password per creare un profilo personale e ottenere accesso completo alle varie funzioni.
Grazie alla semplicità dell'interfaccia, Marta può in qualsiasi momento interrompere la navigazione, sapendo che potrà tornare in seguito.

2.2 UTENTE REGISTRATO

2.2.1 Segnalazione di notizie sospette

Dopo essersi registrato, **Luca** accede con le proprie credenziali alla piattaforma **FakeNews Checker**.
Mentre scorre le ultime notizie pubblicate, nota un articolo ambiguo e decide di segnalarlo per avviare una verifica.

Luca clicca sul pulsante **"Segnala come sospetta"**. Il sistema apre un modulo di segnalazione dove deve compilare alcuni campi obbligatori: titolo dell'articolo, breve descrizione della motivazione e un link a una fonte ritenuta più affidabile.

Dopo aver inserito tutte le informazioni, Luca conferma l'invio. Il sistema registra la segnalazione e mostra un messaggio di conferma ("Segnalazione inviata con successo"). Nella sua area personale, l'utente può consultare in qualsiasi momento l'elenco delle segnalazioni effettuate.

Qualora inserisse un URL errato o non valido, il sistema lo avviserebbe immediatamente con un messaggio d'errore, suggerendo di controllare la fonte indicata prima di procedere nuovamente all'invio.

Grazie a questa funzionalità, Luca contribuisce attivamente al controllo dell'informazione, collaborando alla lotta contro la disinformazione online.

2.3 AMMINISTRATORE DELLE VERIFICHE

2.3.1 Verifica e aggiornamento dello stato di una notizia

Chiara, una delle amministratrici del team di verifica di **FakeNews Checker**, accede quotidianamente al pannello di controllo del sistema per gestire le segnalazioni inviate dagli utenti registrati.

Dopo il login, il sistema le presenta la lista completa delle segnalazioni in attesa di revisione, ognuna corredata da ID, titolo, link dell'articolo, descrizione della segnalazione e nome dell'utente che l'ha inviata.
Selezionandone una, Chiara accede alla scheda dettagliata e inizia la fase di verifica, consultando fonti certificate come agenzie di stampa, giornali riconosciuti e piattaforme di fact-checking.

Durante il processo può aggiornare lo stato della notizia in base alle evidenze raccolte:

- se l'articolo risulta fondato su fonti attendibili, imposta lo stato su **"Verificato"** (contrassegnato in verde);
- se invece il contenuto è falso, lo marca come **"Non attendibile"**, e il sistema provvede automaticamente alla rimozione dalla sezione pubblica;
- nel caso in cui le informazioni non siano ancora sufficienti, può lasciare la notizia con stato **"In verifica"**, mantenendo il ticket aperto fino a ulteriori accertamenti.

Una volta completata la procedura, Chiara chiude la segnalazione con l'esito definitivo.

2.4 AMMINISTRATORE TECNICO

2.4.1 Gestione tecnica del sistema

Alessia, amministratrice tecnico del progetto **FakeNews Checker**, ha il compito di garantire il corretto funzionamento della piattaforma.
Ogni giorno accede alla dashboard di monitoraggio per controllare lo stato dei server e del database.

In caso di anomalie, Alessia interviene per individuare la causa del problema. Se necessario, effettua un riavvio dei servizi principali (server o database), assicurandosi che la piattaforma torni pienamente operativa.
Quando vengono rilasciati nuovi aggiornamenti, Alessia li testa prima in un ambiente di sviluppo locale per evitare malfunzionamenti.

Oltre alla manutenzione ordinaria, gestisce anche le richieste di supporto tecnico provenienti dagli altri amministratori o dagli utenti, come problemi di caricamento pagine o accesso negato.

Grazie a queste attività di supervisione costante, Alessia garantisce che **FakeNews Checker** resti stabile, sicuro e sempre disponibile per tutti gli utenti, consentendo la continuità delle verifiche e della consultazione delle notizie.

3 FUNCTIONAL REQUIREMENTS

3.1 UTENTE NON REGISTRATO

RF1
Il sistema deve consentire agli utenti non registrati di consultare le notizie pubblicate sulla piattaforma.
RF2
Il sistema deve permettere la visualizzazione dello stato di verifica di ciascuna notizia (*Verificata*, *In verifica*, *Non attendibile*).
RF3
Il sistema deve consentire agli utenti non registrati di utilizzare la barra di ricerca per cercare le notizie per titolo.
RF4
Il sistema deve offrire un collegamento alla sezione di registrazione e accesso per permettere agli utenti non registrati di creare un account.

3.2 UTENTE REGISTRATO

RF5
Il sistema deve consentire agli utenti registrati di segnalare una notizia sospetta compilando un modulo con titolo, link e motivazione.
RF6
Il sistema deve permettere agli utenti registrati di inviare articoli o link esterni da sottoporre a verifica.
RF7
Il sistema deve fornire all'utente registrato una sezione personale per visualizzare lo storico delle segnalazioni inviate.
RF8
Il sistema deve consentire agli utenti registrati di modificare le proprie informazioni personali (nome, e-mail, password).

3.3 AMMINISTRATORE DELLE VERIFICHE

RF9
Il sistema deve consentire agli amministratori di visualizzare tutte le segnalazioni ricevute dagli utenti registrati.
RF10
Il sistema deve permettere agli amministratori di aggiornare lo stato delle notizie segnalate (es. *In verifica*, *Verificata*, *Non attendibile*).

RF11
Il sistema deve consentire agli amministratori di approvare, correggere o rimuovere le notizie considerate inaffidabili.
RF12
Il sistema deve fornire agli amministratori un pannello di controllo per consultare ciascuna segnalazione e aggiungerne di nuove se necessario.

3.4 AMMINISTRATORE TECNICO

RF13
Il sistema deve consentire all'amministratore tecnico di monitorare lo stato dei server e del database.
RF14
Il sistema deve permettere all'amministratore tecnico di gestire eventuali errori o malfunzionamenti.
RF15
Il sistema deve permettere l'aggiornamento del software e la gestione delle versioni senza compromettere la disponibilità della piattaforma.

3.5 REQUISITI COMUNI A TUTTI GLI UTENTI

RF16
Il sistema deve consentire a ogni utente autenticato di accedere alla propria area personale per consultare o aggiornare i dati del profilo.
RF17
Il sistema deve consentire l'accesso alla piattaforma da diversi dispositivi (desktop, tablet e smartphone).
RF18
Il sistema deve mostrare messaggi di conferma o errore per ogni operazione eseguita (invio segnalazione, accesso non riuscito, ecc.).

4 NONFUNCTIONAL REQUIREMENTS

USABILITY

RNF1 – Interfaccia semplice e coerente
L'interfaccia deve essere chiara, intuitiva e coerente tra le diverse sezioni del sito, in modo che un utente con competenze digitali di base possa navigare e utilizzare le principali funzioni (consultazione e segnalazione) senza assistenza esterna.

RNF2 – Responsività dell'interfaccia
L'interfaccia grafica deve adattarsi automaticamente a differenti risoluzioni di schermo (desktop, tablet e smartphone) mantenendo piena leggibilità e funzionalità.

RELIABILITY

RNF3 – Integrità e sicurezza dei dati
Le password e le informazioni sensibili degli utenti devono essere memorizzate in modo sicuro utilizzando algoritmi di hashing moderni come **SHA-256**.
RNF4 – Gestione degli errori
Il sistema deve essere in grado di gestire errori e anomalie senza interruzioni improvvise del servizio.

PERFORMANCE

RNF5 – Gestione del carico utenti
La piattaforma deve supportare in modo stabile almeno **500 utenti simultanei**, senza degrado evidente delle prestazioni.

SUPPORTABILITY

RNF6 – Struttura modulare del codice
Il codice dell'applicazione deve essere organizzato in moduli indipendenti per facilitare manutenzioni, correzioni e aggiornamenti futuri. Ogni componente deve poter essere sostituito o migliorato senza modificare l'intero sistema.
RNF7 – Ambiente di esecuzione
Il sistema deve poter essere installato e avviato su server web con database relazionale accessibile da rete Internet.

OPERATION

RNF8 – Monitoraggio
Eventuali errori, malfunzionamenti o tentativi di accesso non autorizzato devono essere registrati automaticamente. Gli amministratori devono individuare problemi o attività sospette.

RNF9 – Manutenzione e aggiornamenti
L'amministratore tecnico deve poter aggiornare la piattaforma senza perdita di dati, garantendo la continuità del servizio e un ripristino completo in caso di guasti.

LEGAL

RNF10 – Conformità al GDPR
La raccolta e il trattamento dei dati personali devono essere conformi al **Regolamento Europeo (GDPR)**, assicurando consenso esplicito dell'utente e trasparenza nell'utilizzo dei dati.

5 TARGET ENVIRONMENT

- **Tipo di sistema:** piattaforma web.
- **Ambiente di esecuzione:** browser web (Google Chrome, Mozilla Firefox, Safari, Edge).
- **Tecnologie previste:** linguaggi web standard (HTML, CSS, Java); database relazionale per la gestione dei dati.
- **Accesso:** tramite rete Internet, disponibile su dispositivi desktop e mobile.

6 DELIVERABLE & DEADLINES

DELIVERABLE	DESCRIZIONE	DATA DI CONSEGNA
Requisiti e casi d'uso	Identificazione dei requisiti funzionali e non funzionali e definizione dei principali casi d’uso.	28/10/2025
Requirements Analysis Document	Analisi dettagliata dei requisiti del sistema	11/11/2025
System Design Document	Documento di progettazione architetturale: struttura three-tier del sistema	25/11/2025
Specifica delle interfacce dei moduli del sottosistema da implementare: Object Design Document	Descrizione delle classi, dei metodi e delle interfacce relative al sottosistema scelto per l’implementazione.	16/12/2025
Piano di test di sistema e specifica dei casi di test per il sottosistema da implementare	Piano di test del sistema e specifica dei casi di test relativi al sottosistema implementato.	16/12/2025
Object Design Document	È il documento che descrive la progettazione di basso livello del sistema, cioè come viene effettivamente implementato il software	07/01/2026
Documenti di esecuzione del test	Documenti che descrivono come è stato testato il software per verificare che funzioni correttamente	09/01/2026
Consegna finale	Progetto finale: FakeNews Checker	11/01/2026