TIR
TEST INCIDENT REPORT
ModuLink

Riferimento	NC08_TIR_ver.1.0
Versione	1.0
Data	20/01/2026
Destinatario	Studenti di Ingegneria del Software 2025/26
Presentato da	Buzi Arjel, Carpentieri Daniele, Chikviladze Aleksandre, Cito Roberto.
Codice Gruppo	NC08
Approvato da	

Revision History

Data Versione		Descrizione	Autori
20/01/2026	0.1	Prima stesura	Daniele
20/01/2026	1.0	Fine Stesura Definitiva	Aleksandre

Team members

Nome	Ruolo nel progetto	Acronimo	Informazioni di contatto
Roberto Cito	Team Member	RC	r.cito@studenti.unisa.it
Daniele Carpentieri	Team Member	DC	d.carpentieri8@studenti.unisa.it
Aleksandre Chikviladze	Team Member	AC	a.chikviladze@studenti.unisa.it
Arjel Buzi	Team Member	AB	a.buzi@studenti.unisa.it

Sommario

1. INTRODUZIONE

1.1 Scopo del Documento

Il presente documento costituisce il **Test Incident Report (TIR)** relativo al progetto **ModuLink**. Lo scopo di questo rapporto è documentare in modo dettagliato ogni anomalia, difetto o comportamento imprevisto (Bug) riscontrato durante le fasi di Testing di Sistema e di Regression Testing. Il documento funge da registro ufficiale degli incidenti, tracciando per ciascuno:

- La descrizione del problema.
- La severità dell'impatto.
- Lo stato della risoluzione (Aperto/Chiuso). Questo report è complementare al *Test Summary Report (TSR)* e fornisce l'evidenza oggettiva delle correzioni apportate prima del rilascio finale.

1.2 Scopo del Prodotto

ModuLink è una piattaforma web modulare di tipo SaaS (*Software as a Service*) progettata per la gestione integrata dei processi aziendali. Il sistema consente alle aziende di configurare il proprio ambiente di lavoro installando specifici Moduli (es. GTM per i Task, GDM per il Magazzino, GCA per il Calendario) e gestisce l'accesso multi-tenant sicuro tramite un sistema di ruoli (RBAC). L'obiettivo dei test è stato validare che tutte le funzionalità critiche, incluse le logiche di business e i vincoli di integrità dei dati, rispondano ai requisiti definiti.

1.3 Acronimi e Definizioni

Acronimo	Definizione
TIR	*Test Incident Report*. Documento di segnalazione delle anomalie.
TSR	*Test Summary Report*. Documento riepilogativo dell'attività di test.
TCSD	*Test Case Specification Document*. Specifica dei casi di test.
SUT	*System Under Test*. Il sistema oggetto del test (ModuLink v1.0).
Bug	Difetto o errore nel codice che causa un comportamento non conforme ai requisiti.
Severity	Grado di gravità di un incidente (es. Bloccante, Critico, Minore).

1.4 Documenti di Riferimento

La stesura di questo report fa riferimento alla seguente documentazione approvata:

- [RAD] Requirements Analysis Document v1.4
- [SDD] System Design Document v1.2
- [TPD] Test Plan Document v0.5
- [TCSD] Test Case Specification Document v0.5
- [TSR] Test Summary Report v1.0

2. AMBIENTE DI ESECUZIONE

Questa sezione descrive la configurazione hardware e software utilizzata per l'esecuzione dei test in cui sono stati rilevati gli incidenti.

2.1 Hardware e Software

I test sono stati eseguiti in un ambiente locale controllato, con le seguenti specifiche:

- **Server Application:** Apache Tomcat (Embedded in Spring Boot 3.5.6).
- **Database:** MySQL Server 8.0 (con dataset di test pre-popolato).
- **Java Runtime:** JDK 17.
- **Browser Client:**
    - Google Chrome (versione 120+).
    - Mozilla Firefox (versione 121+).
- **Sistema Operativo:** Windows 10/11 (64-bit).

2.2 Strumenti di Testing

Per l'esecuzione, il tracciamento e l'automazione dei test sono stati impiegati i seguenti strumenti:

- **JUnit 5:** Per l'esecuzione dei Test di Unità e Integrazione sul backend.
- **Selenium IDE:** Per l'automazione dei Test di Sistema (registrazione e riproduzione interazioni utente su browser).
- **JaCoCo:** Per la misurazione della copertura del codice (*Code Coverage*).

3. TEST INCIDENT REPORT

In questa sezione sono riportati i dettagli delle anomalie riscontrate durante l'esecuzione dei Test Case. Ogni incidente è stato tracciato, analizzato e risolto dal team di sviluppo.

3.1 Metodologia di Segnalazione

Gli incidenti sono classificati secondo i seguenti criteri:

- **ID Incidente:** Identificativo univoco (es. *TI_001*).
- **Test Case Rif.:** Il caso di test che ha fallito e ha generato l'incidente.
- **Severità:**
  - *Alta:* Blocca una funzionalità critica o compromette l'integrità dei dati.
  - *Media:* Funzionalità parzialmente compromessa o comportamento non conforme alle specifiche.
  - *Bassa:* Difetto minore (es. estetico) che non impatta l'operatività.
- **Stato:**
  - *Aperto:* Anomalia in attesa di correzione.
  - *Risolto (Closed):* Correzione applicata e verificata con successo (Regression Test).

3.2 Riepilogo Incidenti

La seguente tabella riassume gli incidenti emersi durante la prima iterazione di test (Data: 12/01/2026). *Nota: Alla data di rilascio del presente documento (22/01/2026), tutti gli incidenti risultano **RISOLTI**.*

ID Incidente	Test Case Rif.	Modulo	Descrizione Breve	Severità	Stato
TI_001	TC2_GDU.1	GDU	Sicurezza: Password utente accettata anche se < 8 caratteri	Alta	**Risolto**
TI_002	TC7_GDM.1	GDM	Dati: Inserimento prodotti con prezzo negativo o nullo	Alta	**Risolto**
TI_003	TC5_GTM.1	GTM	Logica: Creazione Task con scadenza nel passato	Media	**Risolto**

3.3 Dettaglio Anomalie Riscontrate

Di seguito vengono analizzati nel dettaglio gli incidenti critici risolti.

INCIDENTE TI_001 – Sicurezza Password

Campo	Dettaglio
Data Rilevamento	12/01/2026
Tester	Arjel Buzi (AB)
Descrizione	Durante la registrazione di un nuovo utente, il sistema accettava password insicure (es. "123") violando il requisito di sicurezza che impone una lunghezza minima di 8 caratteri.
Input Fornito	Password: "pass" (4 caratteri).
Risultato Atteso	Messaggio di errore: "La password deve contenere almeno 8 caratteri". Registrazione bloccata.
Risultato Ottenuto	Utente creato con successo e reindirizzato al login.
Analisi Tecnica	Mancata annotazione di validazione `@Size(min=8)` nel DTO `RegisterResponsabileForm.java`.
Azione Correttiva	Aggiunta annotazione di validazione e aggiornamento del metodo nel `RegisterController`.
Esito Retest	**PASSED** (22/01/2026). Il sistema ora respinge password brevi.

INCIDENTE TI_002 – Integrità Prezzo Prodotto

Campo	Dettaglio
Data Rilevamento	12/01/2026
Tester	Daniele Carpentieri (DC)
Descrizione	Nel modulo Magazzino, era possibile inserire nuovi prodotti specificando un prezzo negativo (es. -50.00€), causando incongruenze nei totali contabili.
Input Fornito	Nome: "Monitor", Prezzo: -100.0
Risultato Atteso	Blocco dell'inserimento e alert: "Il prezzo deve essere maggiore di zero".
Risultato Ottenuto	Prodotto salvato con prezzo negativo.
Analisi Tecnica	Assenza di controllo sul segno del valore nel ProdottoService.
Azione Correttiva	Implementato controllo if (prezzo <= 0) nel metodo inserisciProdotto del controller GDM.
Esito Retest	**PASSED** (22/01/2026). Il sistema mostra correttamente l'errore di validazione.

INCIDENTE TI_003 – Coerenza Temporale Task

Campo	Dettaglio
Data Rilevamento	12/01/2026
Tester	Roberto Cito (RC)
Descrizione	Il Task Manager permetteva di creare attività impostando una data di scadenza antecedente alla data odierna (retroattiva).
Input Fornito	Data Scadenza: [Data di ieri]
Risultato Atteso	Errore: "La data di scadenza non può essere nel passato".
Risultato Ottenuto	Task creato correttamente con scadenza già passata.
Analisi Tecnica	Logica di confronto date assente nel metodo createNewTask del GTMController.
Azione Correttiva	Aggiunto validatore: if(form.getScadenza().isBefore(LocalDate.now())).
Esito Retest	**PASSED** (22/01/2026). L'inserimento di date passate viene bloccato.