



User Guidelines for Submitting Significant Cyber Threat Notifications

User Guidelines for the notification of Significant Cyber Threat Notifications to the Malta Financial Services Authority through the Licence Holder Portal.

Contents

- 1. Introduction 4
 - 1.1 Accessing the Licence Holder Portal..... 4
 - 1.2 Registering and/or Logging In..... 5
- 2. Notification of a Significant Cyber Threat 7
 - 2.1 Submitting a Significant Cyber Threat Notification..... 7
- 3. Resubmission of a Significant Cyber Threat Notification 10
 - 3.1 Resubmission of Notifications..... 10
- 4. Engaging with the assigned MFSA Analyst through the CRMS 12
- 5. Withdrawing a Significant Cyber Threat Notification 14
- 6. Contacting Us..... 16

Table of Abbreviations

LH Portal

Licence Holder Portal

MFSA

Malta Financial Services Authority

CRMS

Cyber Reporting Management System

1. Introduction

This document provides the necessary guidelines for an Authorised Person to notify on a voluntary basis, Significant Cyber Threats to the Malta Financial Services Authority ('MFSA'), through the License Holder Portal ('LH Portal'). This document should be read in conjunction with Circular titled [Cyber Reporting Management System \(CRMS\)](#) and the following material released alongside these guidelines, available on the MFSA website (Our Work > Supervisory ICT Risk & Cybersecurity):

1. Significant Cyber Threat Notification Process ('the Process Document');
2. Template for Significant Cyber Threat Notifications ('the Template', 'the provided Template').

1.1 Accessing the Licence Holder Portal

The LH Portal is a web-based application which enables all entities, licensed by the MFSA (Authorised Persons) to submit Personal Questionnaires (PQs) access their information, as well as upload regulatory returns/documentation. The LH Portal can be accessed through a web-browser via <https://lhportal.mfsa.mt>.

A project has been created within the LH Portal – the Cyber Reporting Management System (CRMS) – for the submission of Major ICT-Related Incident Reports, Significant Cyber Threats and Information-Sharing Arrangements.

1.2 Registering and/or Logging In

A user is expected to Log-In to the LH Portal to be able to notify Significant Cyber Threats as illustrated in Figure 1.2.1.

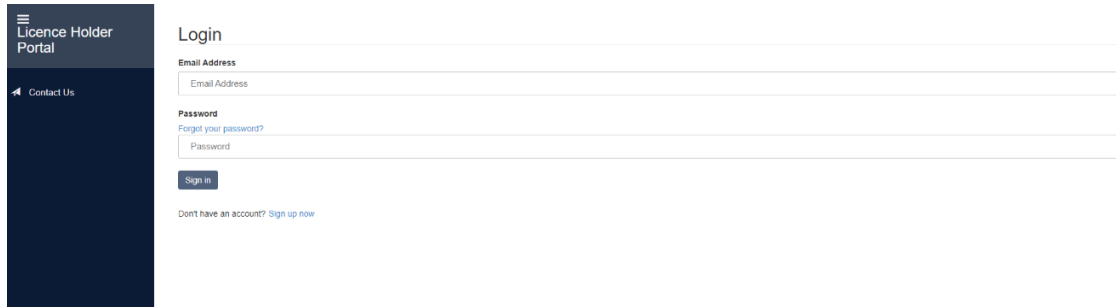
The screenshot shows the 'Licence Holder Portal' interface. On the left is a dark blue sidebar with a 'Contact Us' link. The main content area is titled 'Login' and contains two input fields: 'Email Address' and 'Password'. The 'Password' field has a 'Forgot your password?' link above it. Below the fields is a 'Sign in' button. At the bottom, there is a link for users who do not have an account: 'Don't have an account? [Sign up now](#)'.

Figure 1.2.1 LH Portal Log-In

Access to the CRMS is granted to specific users, typically approved Compliance Officers acting for and on behalf of the Authorised Person/s. Users requiring access should initially register on the LH Portal, as illustrated in Figures 1.2.2 and 1.2.3. Once an account is created using the business email address, the designated person is to contact the Supervisory ICT Risk and Cybersecurity Function by sending an email to mirt@mfsa.mt to have the account linked with the CRMS project.

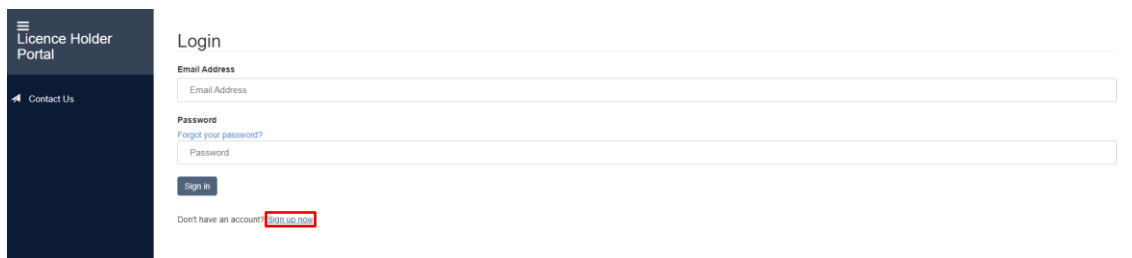
This screenshot is identical to Figure 1.2.1, showing the 'Licence Holder Portal' login page. The 'Sign up now' link in the text 'Don't have an account? [Sign up now](#)' is highlighted with a red rectangular box.

Figure 2.2.2 LH Portal Registering an Account (1)

Register an account

If you are registering an account to complete a **Personal Questionnaire**, kindly use a private email and not a corporate email.

Verification is necessary. Please click Send button.

Email Address

Send verification code

New Password

Confirm New Password

Document Type

DOCUMENT TYPE ▾

Official Identification Document No

Name

Surname

Create

Cancel

Figure 3.2.3 LH Portal Registering an Account (2)

2. Notification of a Significant Cyber Threat

A Cyber Threat shall be considered as a Significant Cyber Threat where it has met the conditions specified in Chapter III of [Commission Delegated Regulation \(EU\) 2024/1772 of 13 March 2024, supplementing the DORA Regulation with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents](#). Authorised Persons are encouraged to notify Significant Cyber Threats to the Authority.

Notification is expected to occur using the provided Template and in line with the Process Document.

2.1 Submitting a Significant Cyber Threat Notification

Once the user has successfully signed in and accessed the CRMS page, the user is to select the 'Significant Cyber Threats' button (see Figure 2.1.1).

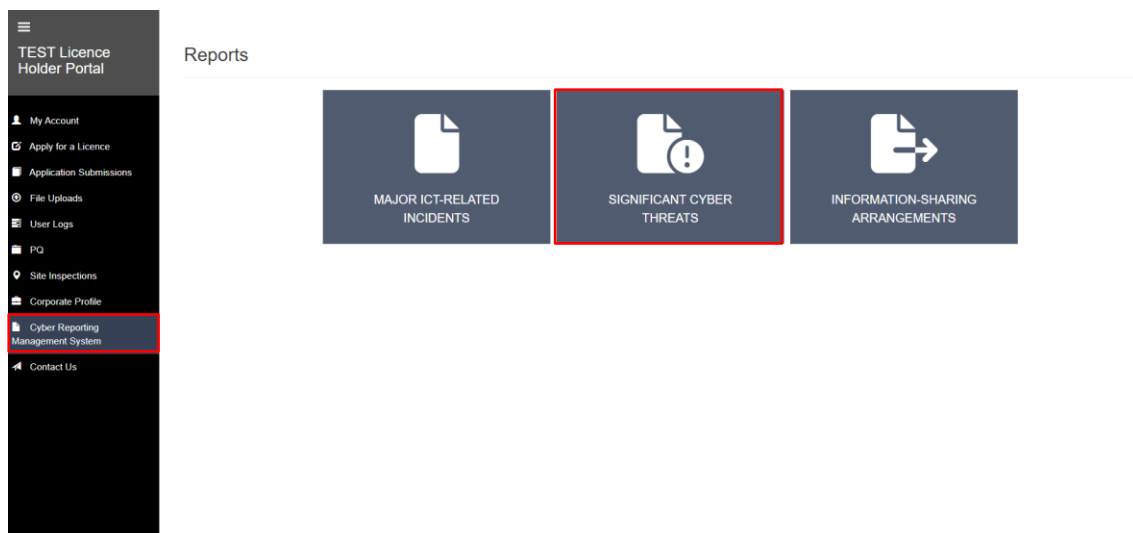


Figure 2.1.1: CRMS Main Page

The user will then be redirected to the Significant Cyber Threats main page and is to select the 'Issue Notification' button (see Figure 2.1.2).

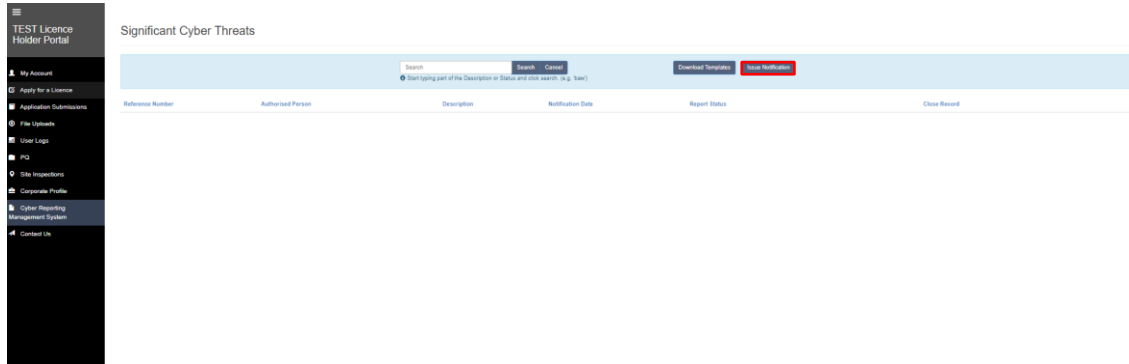


Figure 2.1.2: Significant Cyber Threats Main Page

The submission page of the Significant Cyber Threat notification will be displayed, and is split into three (3) sections (see Figure 2.1.3).

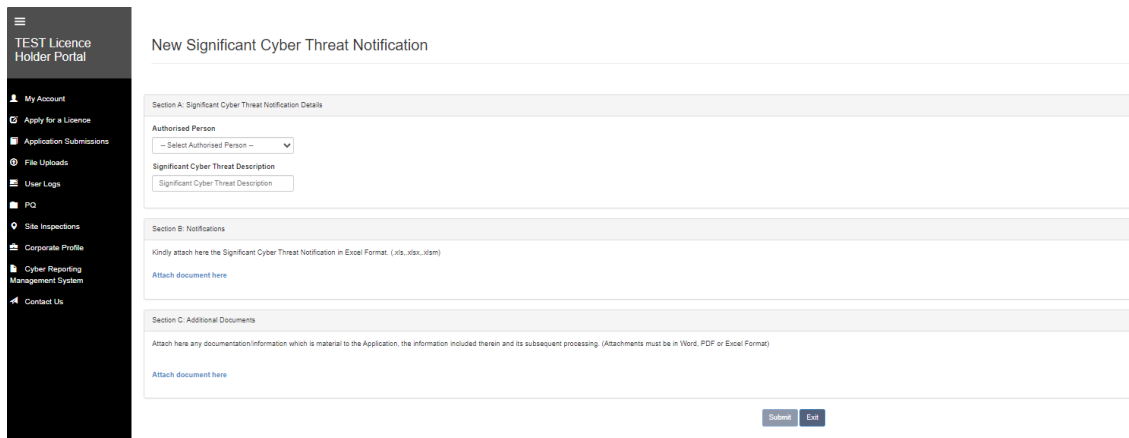


Figure 2.1.3: Significant Cyber Threats Notification Page

Section A: Significant Cyber Threat Notification Details

The user is to select the 'Authorised Person' subject to the notification, from the drop-down list and include a short description of the Significant Cyber Threat within the 'Significant Cyber Threat Description' field.

Section B: Notifications

The user is to upload the Notification using the provided Template by selecting the 'Attach document here' button under Section B.

Section C: Additional Documents (optional)

The user is able to upload any additional documents (in Microsoft Word, Excel or PDF format) in relation to the Significant Cyber Threat by selecting the 'Attach document here' button under Section C.

After completing sections, A, B and C above, the user will then need to select the 'Submit' button located at the bottom of the page. The user will then be redirected to the Significant Cyber Threat notification page where all the information related to the notification is displayed (see Figure 2.1.4).

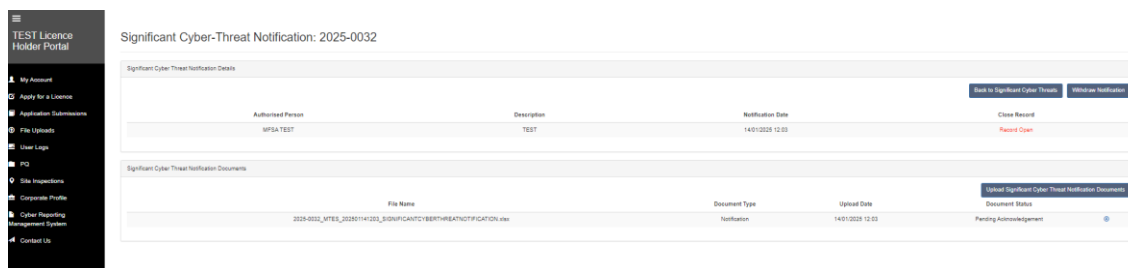


Figure 2.1.4: Cyber Threat Notification Page Notification | Record Page

3. Resubmission of a Significant Cyber Threat Notification

3.1 Resubmission of Notifications

In case the assigned MFSA analyst is not satisfied with the submitted notification (for instance, a submitted notification lacks the necessary completeness, or a template file format has been tampered with), the Authorised Person will be requested to carry out a resubmission. The respective 'Document Status' within the Significant Cyber Threat Notification record will appear as 'Request Resubmission' (see Figure 3.1.1).

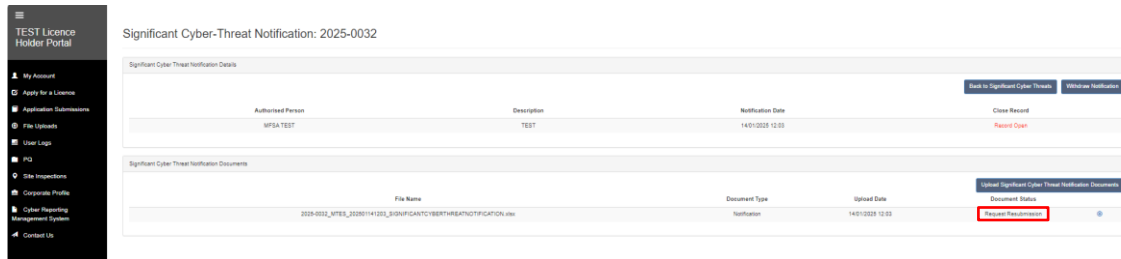


Figure 3.1.1: CRMS Cyber Threat Notification Page | Resubmission

The user will receive an email requesting resubmission and will then need to select the 'Upload Significant Cyber Threat Notification Documents' button to attach and submit the updated version of the respective notification (see Figure 3.1.2).

TEST Licence Holder Portal

My Account
Apply for a Licence
Application Submissions
File Uploads
User Logs
FAQ
Site Inspections
Corporate Profile
Cyber Reporting Management System
Contact Us

Significant Cyber Threat Notification

Section A: Significant Cyber Threat Notification Details

Authorised Person
MPSA.TEST

Incident Report Description
TEST

Section B: Notifications

Kindly attach here the Significant Cyber Threat Notification in Excel Format. (.xls, .xlsx, .xlsm)
2025-032_MTES_202501141203_SIGNIFICANTCYBERTHREATNOTIFICATION.xlsx

[Attach document here](#)

Section C: Additional Documents

Attach here any documentation/information which is material to the Application, the information included therein and its subsequent processing. (Attachments must be in Word, PDF or Excel Format)

[Attach document here](#)

[Submit](#) [Exit](#)

Figure 3.1.2: Resubmission of a Cyber Threat Notification

4. Engaging with the assigned MFSA Analyst through the CRMS

Authorised Persons may engage with the assigned MFSA Analyst through the CRMS within the LH Portal in relation to a Significant Cyber Threat Notification by clicking on the 'Contact' icon on the far right of the Significant Cyber Threat record, as illustrated in Figures 4.1-4.3, which provides a chat box facility.

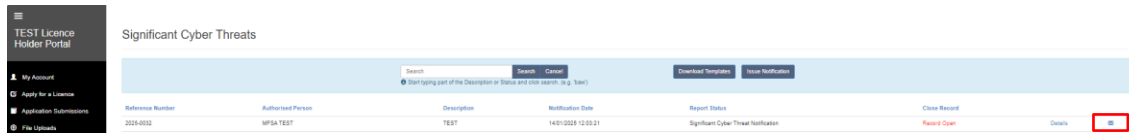


Figure 4.1: Significant Cyber Threats Main Page

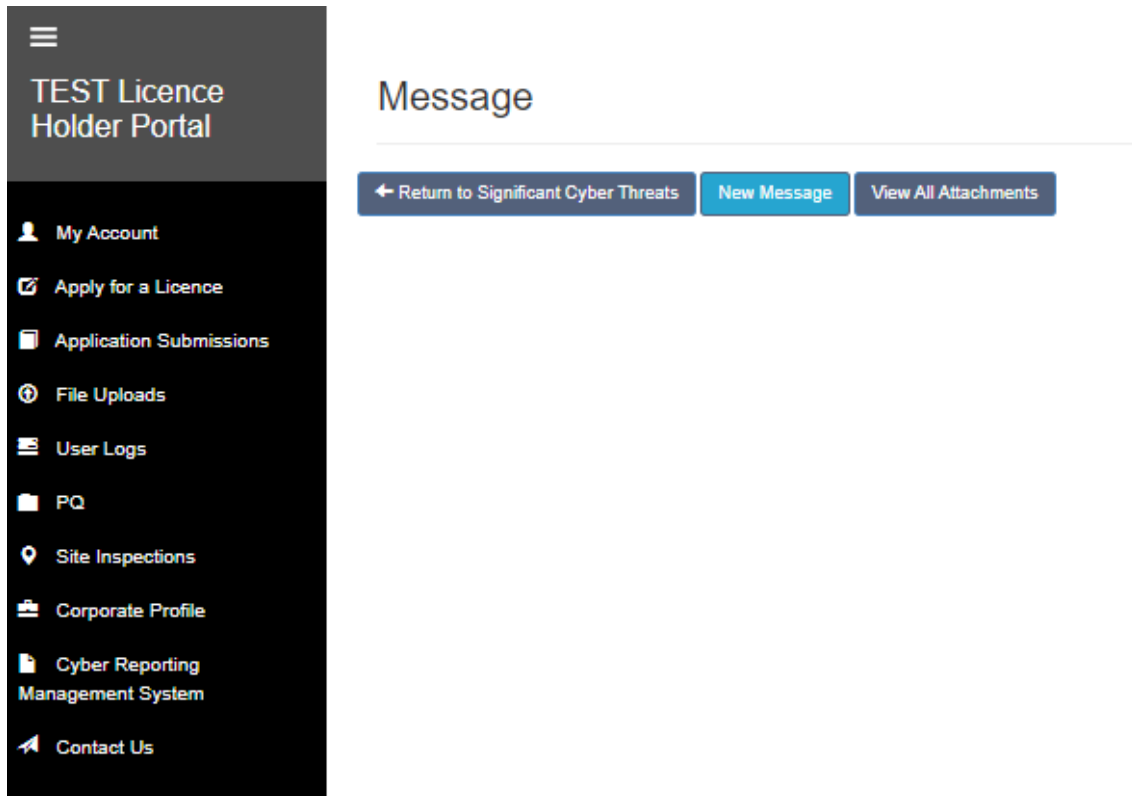


Figure 4.2: Significant Cyber Threats 'Message User' Button

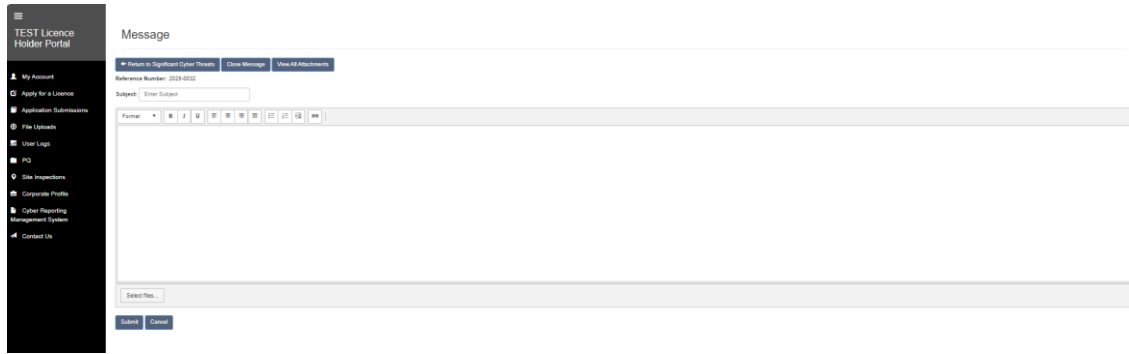


Figure 4.3: Significant Cyber Threats Contact Page

5. Withdrawing a Significant Cyber Threat Notification

If a Cyber Threat notification, upon further investigation, is afterwards determined to not classify as 'significant', the Authorised Person has the facility to withdraw its submission through the CRMS.

The user needs to select the 'Details' button (see Figure 5.1) and will subsequently be redirected to the Cyber Threat Notification Page.

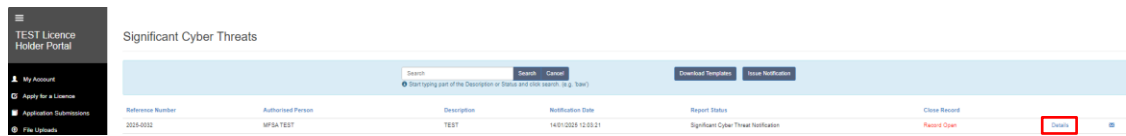


Figure 5.1: Significant Cyber Threats Main Page

The user will then need to select the 'Withdraw Notification' button as illustrated in Figure 5.2.

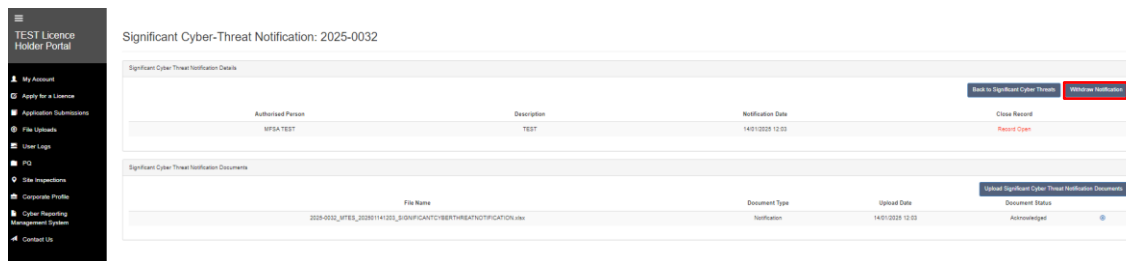


Figure 5.2: Significant Cyber Threats Record Page

The user will get a pop-up notification (see Figure 5.3) to provide a valid reason for withdrawal within the text box provided, before pressing the 'Withdraw Notification' button.

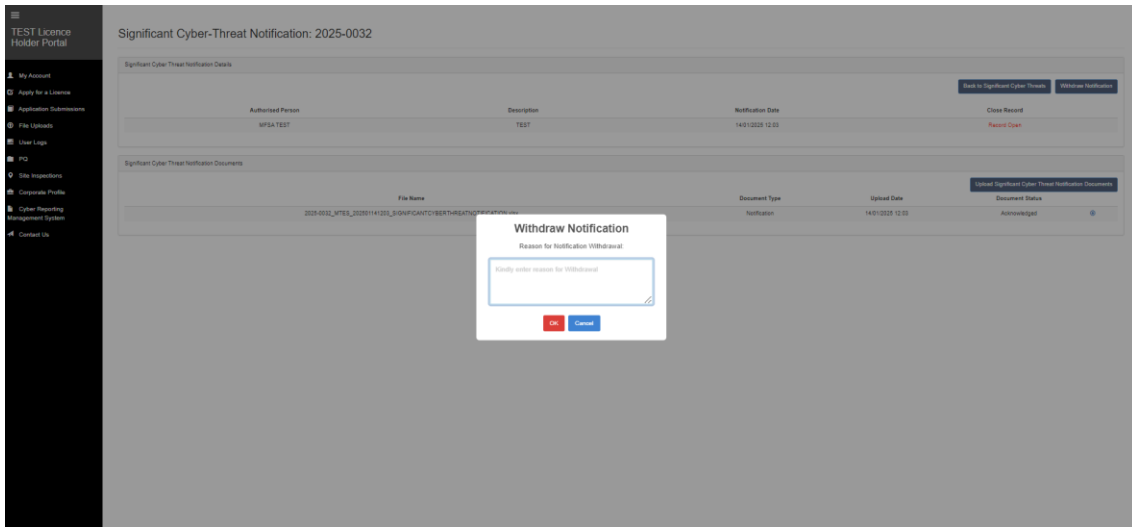


Figure 5.3: Cyber Threat Withdrawal Pop-Up Notification

Following the withdrawal of the notification, the CRMS will automatically update the notification record as seen in Figures 5.4 and 5.5.

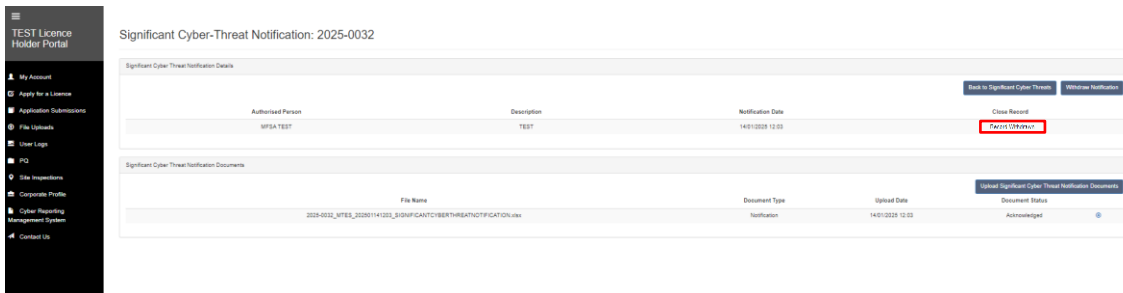


Figure 5.4: Cyber Threat Record Page

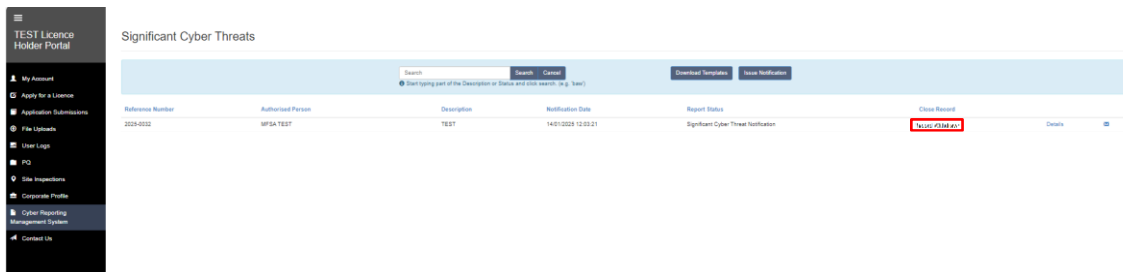


Figure 5.5: Cyber Threats Main Page

6. Contacting Us

In case of any difficulties, do not hesitate to contact the Supervisory ICT Risk and Cybersecurity (SIRC) Function by calling on +356 2548 5260 or by sending an email to mirt@mfsa.mt.