The Lighthouse Case Management System

Get everything you need to track hotline reports from beginning to end in one easy-to-use online tool!

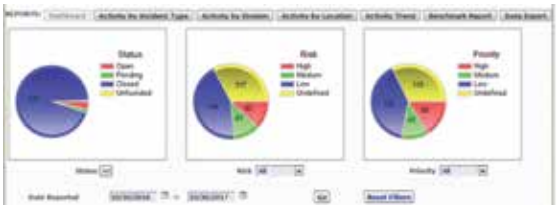
For most organizations, keeping track of hotline reports can be a daunting challenge. Overlooked or missing information can lead to inefficient investigations and leave you vulnerable to potential litigation. Lighthouse's state-of-the-art Case Management System (CMS) allows you to keep track of all report activities from the time an incident is reported all the way through to its resolution. Best of all, there's no additional cost to your company.

Before using CMS for the first time, please take a few minutes to review the help tutorial found at the following link: http://www.lighthouse-services-cms.com/Help/index.html

Key CMS Features and Benefits

CMS provides you and the appropriate ethics and compliance personnel with the ability to:

- **View the report online –** You can access report information online even when away from the office. Because the CMS application resides on the Lighthouse server, there is never a need to download software.
- **Assign the incident to a person for investigation –** You'll be able to assign the report automatically to the appropriate individual quickly, and you'll know the right person to contact if you have questions or concerns about any investigation.
- **Assign risk level, priority & status –** This ensures that the most urgent or sensitive cases are given top priority and that all reports are handled in a timely and expeditious manner.
- **Record your follow-up and outcome –** You'll be able to input all actions taken as well as each report's ultimate resolution, which is critical to creating an audit trail.
- **Dialog with reporter –** Under most circumstances, the case investigator or administrator can carry on an anonymous dialog with the reporter, allowing for the continuous exchange of information throughout the course of an investigation.
- **Create and manage reports –** You'll have the capability to develop a variety of reports that can be issued to key personnel within your organization on a "need to know" basis. Your CMS comes equipped with an advanced analytics dashboard with a view to all key metrics and trends and the ability to drill down to details using a comprehensive and easy to understand set of user controls.



- **Attach multiple files to a report –** You can supplement reports by uploading additional files as needed.
- **Collaborate with ease –** CMS allows users to share either detailed or summary information about a report with appropriate personnel or outside parties. Data from CMS is exportable with push-button simplicity. Our message board feature allows creation and dissemination of client generated messages to system users.
- **Link reports –** You can add a Link ID to associate a report with other previously received reports you identify as having similar issues.

CMS: Designed with the End-User in Mind

CMS is designed with you, the end-user in mind. The numerous user-friendly features save you time, money and hassles while increasing the efficiency of your investigations.

LIGHTHOUSE
Obtaining information. Delivering solutions.

LIGHTHOUSE SERVICES, Inc.
1710 Walton Road, Suite 204, Blue Bell, PA 19422
215.884.6150 | 844-709-6000 lighthouse-services.com

IN A NUTSHELL

Here are just a few of the CMS features and capabilities:

- View the report online
- Assign the incident to a person for investigation
- Assign Risk Level, Priority & Status
- Record your Follow-up and Outcome
- Dialog with Reporter
- Create and manage reports
- Attach multiple files to a report
- Collaborate with ease

Here's how easy CMS is to operate

To access the system, log on to the CMS website by clicking on this link:

http://www.lighthouse-services-cms.com

STEP ONE: Log In

CMS will then prompt you to enter your unique user ID (your email address) and password.

STEP TWO: Visit the Nerve Center (The Incident Reports Tab)

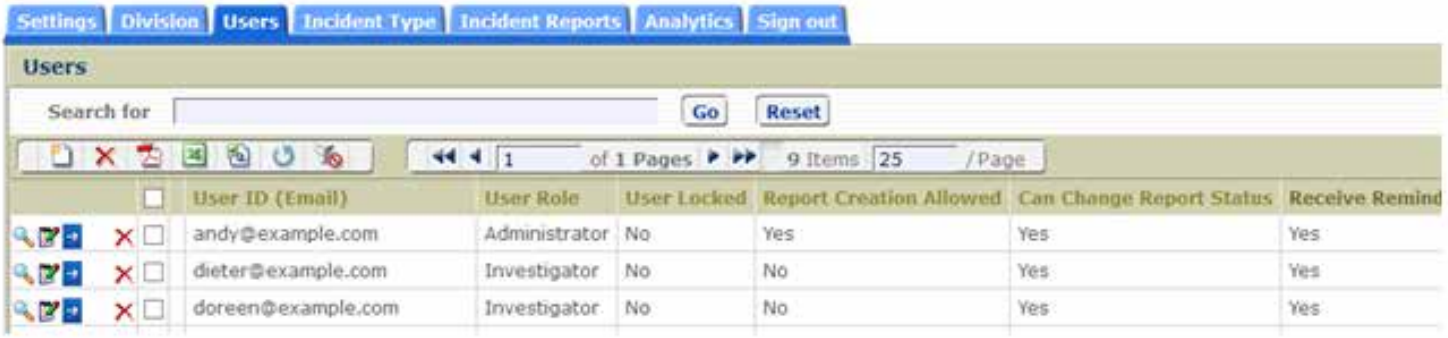
Once you have successfully logged on, CMS will open in the Incident Reports tab, the "nerve center" of the system. From here, you can easily manage all reported cases. Each incident is assigned a unique report number, and the built-in filters allow you to manage cases when using fields such as date, incident type, risk level, priority, status, nature of report, or by using a keyword. By placing your cursor over an object in the application, a pop-up balloon showing a description of the function will appear.

LIGHTHOUSE
Obtaining information. Delivering solutions.

LIGHTHOUSE SERVICES, Inc.
1710 Walton Road, Suite 204, Blue Bell, PA 19422
215.884.6150 | 844-709-6000 lighthouse-services.com

Add New Administrators and Investigators/non-Administrators Using the Users Tab

CMS also allows you to designate individuals as Administrators who have access to all case records, and Investigators/non-Administrators who have access only to those records assigned to them by the Administrator. This feature helps you optimize the effectiveness of CMS by providing an additional level of oversight and control.



Defined User Roles

The system has two levels of users: Administrators, who have access to all records, and Investigators/non-Administrators, who are assigned to individual records by the Administrator. Administrators set up Investigator/non-Administrator profiles are dynamic, user access and permissions can be modified based on the individual user's needs. However, by default, Investigators/ non-Administrators have the ability to access only those records assigned to them. Records can be assigned to one or more Administrators or Investigators by clicking on the [assign user] icon in the Incident Reports tab.

Company Administrators have access to the entire system without impediment.

- They can add or delete users, change user roles and manage user profiles.
- They can add and delete different divisions within your company as necessary.
- They can access all incident reports, assign investigators, track progress, dialog, add files, etc.

Investigators/non-Administrators profiles are dynamic and can be modified based on a user's needs. However, by default Investigators/ non-Administrators only have access to the Incident Report tab.

- They can only investigate, track progress, dialog, add files, etc.
- They cannot add investigators to reports
- They cannot modify system settings

Other Important Features

Dialog Capabilities – Under most circumstances both Administrators and Investigators will be capable of engaging in anonymous dialog with a reporter. All Administrators and any Investigators assigned to an incident report will be copied on dialog emails, unless your organization elects to omit unassigned Administrators. However, if there is no assigned Investigator and Administrators have elected to not view dialog emails, reporter emails will be sent to all Administrators by default.

Manage Custom Fields – CMS allows an administrator to define up to three client defined fields for a report. These custom fields will appear on the Add/ Edit/Show Incident Report pages and will be included in exports of incident report data. The following types of custom fields are available:

- Numeric - Integer
- Number - Decimal (2 decimal places)
- Numeric - Currency (2 decimal places)
- Date
- Text (maximum 255 characters)
- Dropdown List

Audit Trail – The CMS provides you with fields for your Follow-Up and Outcome notes. These fields are available for entering progress notes and logging investigative activities. Username and time and date of entries are displayed whenever text is added in these fields. After entering and saving data into these fields it cannot be modified or removed. Additionally, the system keeps track of every change to a record via an audit interface.

Incident Type Dropdown – Freeform text entry is available to use for every Incident Type.

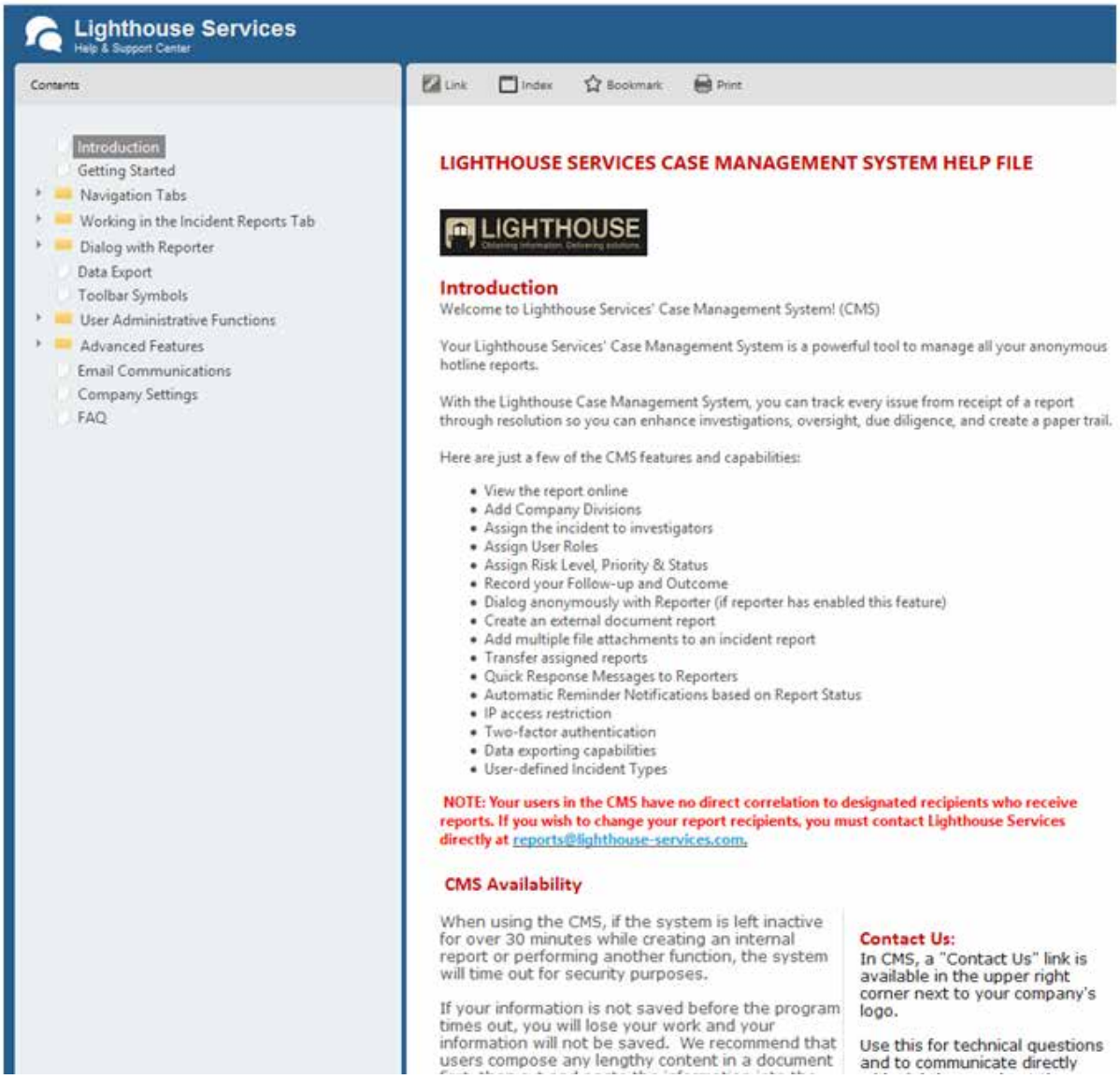
Easily and Quickly Respond to a Reporter – Quick Response Messages are available in the Dialog page. Company users have access to a library of messages that can be quickly sent to/saved for a reporter from the Dialog page. With a few clicks of their mouse, a user can choose which message to send to the reporter.

Create Reports Not Submitted through Lighthouse – CMS gives you the capability to create reports for any incident, even those not reported through the Lighthouse system.

Web API Access – With CMS API enabled clients can initiate remote transactions seamlessly between systems to query the CMS and add incident reports.

Investigator Oversight – Reminder notification emails send configurable email messages to CMS users assigned as investigators on a case. When the feature is enabled, users assigned to a case will receive reminder notification emails when the status of an incident report remains unchanged for a specified period of time.

Convenient Help Tutorials – With CMS, help is never more than a mouse click away. By visiting our help site at http://www.lighthouse-services-cms.com/Help/index.html you will gain access to a variety of menu items that will enhance your user experience.



LIGHTHOUSE SERVICES, Inc.
1710 Walton Road, Suite 204, Blue Bell, PA 19422
215.884.6150 | 844-709-6000 lighthouse-services.com

Customizing Your Lighthouse CMS Site

Your Case Management System will be pre-configured with information that you will provide us in your Service Agreement. The system comes with the following default configurations.

Function	Default Setting	Description
Allow Locations to Be Associated with Divisions	**OFF**	This feature enables an administrator or user with Add/Edit Division permission to associate Locations to one or more Divisions. This will provide filtering of Locations when a Division is chosen on the Add and Edit Incident Report pages.
Suppress Report/Dialog in Emails	**OFF**	This feature allows an Administrator to suppress all dialog and report content within an email from the CMS. By default, report text and dialog are included in the content of CMS emails. If this feature is enabled, emails generated by the CMS between the Company and the Reporter or Lighthouse will only indicate the case number and the sender (Lighthouse or reporter). No other information will be included in the email. The Company would then need to sign in to the CMS to view any dialog or report content.
New Incident Report Email Notification	**OFF**	This feature enables an Administrator to be notified via email when a new incident report has been added to the CMS.
Dialog Copy Administrators	**ON**	This feature allows Administrators to determine if they will receive a copy of dialog updates between the reporter or Lighthouse and the company. When this setting is enabled, the Administrator and all assigned investigators will receive an email when the reporter or Lighthouse enters dialog. When this setting is not enabled, only the assigned investigators are sent an email. Note: Regardless of this setting, all administrators are sent an email when no one is assigned to the report.
Email Status Change to Administrator	**OFF**	When enabled Administrators are notified of an incident report status change. If no Administrator has been assigned to a report all Administrators are notified.
Allow Deletion of Files Uploaded by Company	**ON**	This features allows an Administrator to permit or prevent users from deleting files uploaded by the company for incident reports. This feature provides users with the capability to delete company-uploaded files for incident reports.
Populate Sender Field on Emails	**ON**	This feature allows an Administrator to receive bounce back messages on failed emails to a user. If this feature is not enabled, the Administrator will not receive any notification that a CMS generated email to a user has failed. This feature may need to be disabled if the company's SPAM rules are stringent and will not allow the Sender field to be an email address from their own domain.
Restrict Access to CMS Via IP Address	**OFF**	This feature allows an Administrator to restrict access to CMS via IP Address. If enabled only company specified IP addresses will be able to access CMS.
Enforce Lockout On Unsuccessful Login Attempts	**OFF**	This feature provides the Administrator with the ability to lock a user's account if the user has 5 consecutive failed login attempts. If this feature is enabled, a user's account will be locked after 5 consecutive failed login attempts. The user's account can only be unlocked by an Administrator or Lighthouse. If this feature is not enabled, a user will be presented with a CAPTCHA challenge-response test after 5 consecutive failed login attempts.
Two Factor PIN Authentication Required	**OFF**	This feature provides the Administrator with the ability to require a PIN during the login process for all users as well as the user's id and password credentials. The randomly generated PIN will be sent to the user's email address.
'Division' Field Name		This feature enables an Administrator to change the name of the 'Division' field in CMS. The text in this field will appear on all pages and exports in place of the default field name 'Division'. This field is limited to 15 characters.

LIGHTHOUSE SERVICES, Inc.
1710 Walton Road, Suite 204, Blue Bell, PA 19422
215.884.6150 | 844-709-6000 lighthouse-services.com

Your Company's Confidentiality and Security Is Our Top Priority

The Lighthouse CMS is a cloud-based system that utilizes many levels of security including hardware and software firewalls, secure http access (HTTPS), optional two-factor authentication and IP access restriction, and client-controlled password policies.

The data centers (production and disaster recovery) are located in secure, 24hr-monitored data centers. Our data center provider, SingleHop LLC, is SOC2 compliant and utilizes many security protocols in their data centers including motion sensors, closed circuit video, anti-tailgating measures, security guards at all points of entry, escorting visitors at all times, walls extending from ceiling to floor, and alarms on all exterior windows and doors. Our servers are under a strict maintenance schedule for OS patch and 3rd party software updates.

Our data centers server is co-located in a SOC 2 certified facility that is equipped with proximity security badge access. Our servers are housed in a secure facility and are equipped with:

- Multiple Internet backbone connections
- Automatic fail-over through alternate secure connection
- All servers are protected with RAID drive arrays
- Secure, internally networked, high-speed data transmission between data centers
- 3 independent A/C feeds and robust UPS resources
- Cisco Systems 10G network
- Cisco Guard DDOS protection
- Geographically redundant DNS
- TippingPoint IPS/IDS protection
- Arbor Peakflow traffic analysis
- Arbor Atlas Global Traffic Analyzer
- Automated IP routing and management
- Server to Internet speeds up to 1 Gigabit
- ESET and McAfee Business-Class Anti-Virus

All of our servers are monitored and protected using Alert Logic Intrusion Detection software to identify and eliminate malicious external traffic to our servers. Lighthouse also conducts penetration and vulnerability testing using Veracode software which allow Lighthouse to shore up any system or network deficiencies to protect our clients' data.

Data at rest within our CMS is encrypted using AES 256-bit encryption and data in transit is encrypted using HTTPS. All production database backups are encrypted and stored at a distant, separate data center. Access to our servers by Lighthouse personnel requires VPN access, two-factor authentication and complex credentials. Client access to their CMS requires complex credentials that are client-configured. Clients may also use extended security features of the CMS by enabling two-factor authentication and IP access restriction. User credentials are stored in the CMS using a 256-bit, one-way encryption algorithm. User are also notified of multiple login failures, requests for password changes and notification when their passwords have been changed. Clients may also enable an option to lock out user accounts after multiple login failures. Emails automatically generated from the CMS are encrypted in transit using TLS/SSL.

The following features in the CMS provide our clients with additional security measures:

- Account locking allows Administrator the ability to lock out specific user accounts
- Two-factor authentication requires users provide a randomly generated PIN for each session
- Customizable password requirements including password complexity and expiration rules
- Customizable session timeout rules and email link expiration settings
- Client enabled management of IP addresses with permission to access their CMS
- Enforce lockout on unsuccessful login attempts gives the Administrator the option to lockout a user or require them to respond to a CAPTCHA challenge
- Sign on access log lets users view a history of their previous sessions including IP address.

CMS: The Cost-Free Way to Optimize Your Investigations

With CMS, there's no need to be overwhelmed by or worry about the mishandling of a high volume of hotline reports. Make the most of your Lighthouse Services reporting hotline by using CMS to manage your reporting and investigation process. Don't leave anything to chance.