Governance Risk & Compliance	Policy/Procedure Number:	ADM.03
SVP, Governance, Risk & Compliance	Effective Date:	12-07-2021
	Approval Date:	08-26-2019
Risk Reporting & Escalation Policy	Revision Date:	06-02-2021
	Replaces/Retires Policy Number:	
	Pages:	**1** of **4**

Our Family of Companies

SCOPE:

This policy applies to Catalight Foundation and its subsidiaries and affiliates (the "Family of Companies" or "FoC") officers, consultants, employees, business associates, vendors, contractors, temporary workers, volunteers, and any agent who does business with or on behalf of the FoC.

RESPONSIBLE PERSONS:

The Office of Governance, Risk & Compliance ("GRC") is responsible for the administration of this Policy.

BACKGROUND and PURPOSE:

The purpose of this policy is to establish a process to report Potential Risk Matters, including any potentially identified issues or questions associated with FoC's Code of Conduct, FoC's policies and procedures, laws and regulations.

The main objective is to minimize/eliminate the loss to the FoC's business in terms of revenue loss, loss of reputation, loss of productivity, and customer satisfaction. This policy is aligned with the FoC's Business Continuity Plan's (BCP) Incident Management procedures ensuring that our clients/customers, business activities, and services do not suffer in any way.

Furthermore, to the extent that there is a potential violation of criminal, civil, or administrative law, it is the intent of this policy to allow matters to be promptly and thoroughly investigated, documented and appropriate corrective actions to be implemented.

DEFINITIONS:

A. "Control" means a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of the FoC's objectives.

B. "Information Privacy" means the FoC policies, standards and practices which ensure that the information or data shared by clients, customers and employees is only used for its intended purpose. Information privacy is also the right of individuals to have control over how their personal information is collected and used.

C. "Information Security" or "Data Security" means the protection of data against loss, modification, or unauthorized disclosure during its input to, storage in, or processing by a computing resource or at any point thereafter.

D. "Potential Risk Matter" means a regulatory compliance or risk concern, information privacy and security concerns, information technology and cybersecurity concerns, notices from state or government offices, and/or other evidence or allegations of violations of the FoC's Code of Conduct, policies and procedures, or laws and regulations.

E. "Risk" means the chance of something happening that will have an impact on the FoC.

F. "Risk Management" means the culture, processes and structures that are directed towards realizing potential opportunities while managing adverse effects.

G. "Third-party" means any individual or entity that the FoC does business with. This may include suppliers, vendors, providers, and business partners such as outside counsel and consultants.

H. "Vendor relationship management" means the managing of relationships with third parties.

POLICY:

Risk Reporting

Risk reporting is a responsibility of all, with specific risk responsibilities being allocated to different groups and levels within the FoC. It is important to have complete and current risk information available as this information assists the FoC to make more informed decisions around both strategic direction and operational objectives.

Whether you are an employee, an officer or director, an independent contractor, or someone who does business with us, we ask that you bring to light good faith concerns regarding the FoC's business practices and report Potential Risk Matters immediately upon discovery or notification of the same.

A. Risk owners of the FoC should actively review, document, test and monitor their internal controls for potential or actual violations of FoC policies or law. Risk owners may, on occasion, identify Potential Risk Matters and must escalate in accordance with this policy.

B. Employees have an obligation to report Potential Risk Matters regardless of how the employee became aware of the Potential Risk Matter to their supervisor – e.g., from an external source, detected by an internal control or an internal assessment.

Risk Escalation

Risk escalation is an important process for ensuring that risks are known and understood by the people with the authority to appropriately manage them. Timely escalation is critical to ensure adequate and independent investigations by the appropriate departments. Timeliness is critical because the FoC may have a legal obligation to disclose escalated matters to government agencies. Failure to do so may expose the FoC to potential legal sanctions.

Roles and Responsibilities:

Group	Responsibilities
CEO	• Review reports • Closely monitor extreme risks • Identify new and emerging risks • Business Continuity
GRC	• Gather risk information across the FoC • Review reports • Prepare reports • Identify new and emerging risks • Provide Regulatory Guidance
FoC FoFos	• Review reports • Communicate key risk issues to other executive forums • Identify new and emerging risks • Business Continuity
Risk Owners	• Monitor and review the risks which they own • Prepare reports for the risks which they own • Provide GRC with information on the risks which they own • Identify new and emerging risks • Business Continuity
FoC Business Heads	• Review reports prepared by GRC • Provide executive support to GRC, for example, requiring timely provision of risk information from the organization to GRC • Identify new and emerging risks

Group	Responsibilities
	• Business Continuity
FoC Leaders and Staff	• Provide risk information to those that request it • Monitor and review risks within their areas • Identify new and emerging risks • Business Continuity

RELATED POLICIES AND STANDARDS:

- Employee Handbook
- Business Continuity Plan Incident Management

ATTACHMENTS:

- Attachment A: Examples of Reportable Potential Risk Matters
- Attachment B: General Guidelines for Escalating Potential Risk Matters
- Attachment C: Guidelines for Managing Expressions of Dissatisfaction & Threats from Third Parties With Whom The FoC Contracts With
- Attachment D: Guidelines for Reputation Management Monitoring and Escalation
- Attachment E: Guidelines for Reporting Information Privacy-Security & Cyber Security Threats
- Attachment F: Guidelines for CAPA

Our Family of Companies

Examples of Reportable Potential Risk Matters

Note: This list contains examples of high-level categories of reportable Potential Risk Matters and is by no means exhaustive. If you have any questions regarding whether a matter is reportable, please contact your direct supervisor or the Compliance HelpLine at 1-833-44-PROTECT (1-833-447-7683).

A "Potential Risk Matter" can be either a single event or a series of related events that involves:

A. A violation of the obligation to provide items or services of a quality that meets professionally recognized standards of health care where such violation has occurred in one or more instances and presents an imminent danger to the health, safety or well-being of a client or places the client unnecessarily in high-risk situations;

B. Expressions of Dissatisfaction and/or Threats from Third Parties;

C. Information Privacy and Information Security concerns;

D. Evidence or allegations of actual or potential violations of federal or state criminal, civil or administrative laws for which significant penalties may be assessed or which may subject a FoC entity to significant litigation risk (e.g., consumer protection laws, securities laws, environmental protection laws, etc.);

E. Notice of a government investigation or inquiry or litigation alleging fraud;

F. Material violation of the FoC's policies;

G. Violation of Centers for Medicare and Medicaid (CMS) Conditions of Participation, Commission on Accreditation of Rehabilitation Facilities (CARF) accreditation standards, or other licensing or accreditation standards;

H. Significant findings identified by FoC audits or any review conducted by third parties engaged by any FoC entity; OR

I. Other matters or events likely to cause significant reputational or financial harm to the FoC (not all inclusive):

- Client safety, neglect or abuse
- Inappropriate coding
- Inappropriate claims submission
- False or fraudulent documentation matters
- Inappropriate charging/billing
- Inappropriate charge code selection/chargemaster
- Concerns raised by Regional Centers

- Accreditation matters
- HIPAA or Client/Customer Privacy matters
- EMTALA matters
- Cost reporting matters
- Provider Arrangement matters, such as potential violations of the Stark law or Anti-kickback statute
- Correct level of care
- Appropriately licensed staff
- Quality of care matters

J. Threats

A threat is generally any circumstance or event that can adversely impact an organization's IT assets or data. For example, the Cybersecurity Information Sharing Act of 2015 (CISA) broadly defines cybersecurity threats as any actions that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of systems or data (6 U.S.C. § 1501(5)).

Threats are often characterized as attacks or attack types and may also be defined from several perspectives, including:

- Sources or threat actors, such as:
    - negligent or malicious employees who create internal threats; and
    - nation-state actors or hackers or other criminals who create external threats.
- Events or scenarios, such as:
    - data loss or theft, including data exfiltration;
    - errors or omissions;
    - malicious software (malware) infections;
    - hacking, including computer or network intrusions;
    - unauthorized access to data;
    - physical equipment loss or theft;
    - credential theft; and
    - social engineering, for example, email-based attacks like phishing.
- A combination of sources and events.

The FoC also considers natural disasters or human-caused events that may threaten information confidentiality, integrity, or availability, such as fires,

floods, other major weather events, terrorist attacks, and power outages as threats. Because these environmental threats have potentially far-reaching effects, the FoC will address them separately in a formal business continuity, emergency disaster preparedness and disaster recovery planning process.

Our Family of Companies

General Guidelines for Escalating Potential Risk Matters

All Potential Risk Matters must be reported. If you are unclear on whether something should be reported, err on the side of caution and report it. If something is going wrong or it appears that it may not go according to plan, report it.

1. An employee should escalate to their immediate Supervisor, Manager or Director.
2. The Supervisor, Manager or Director who receives the report should immediately report it to their Department or Business Leader.
3. The Department/Business Leader must immediately escalate the report, as appropriate, to the Entity FoFo when help is needed to find a solution to the risk or prevent additional risks.
4. The Entity FoFo will discuss the matter with the appropriate SME(s) to determine the extent of the risk.
5. Escalation to Executive Leadership

   The Entity FoFo will escalate to Executive Leadership when:

   a. Addressing the risk requires decisions/actions (e.g., expenditures) that are beyond what the Entity FoFo is authorized to decide;

   b. The risk cuts across, or may impact, multiple departments and/or FoC Entities, and/or addressing the risk requires action by multiple departments; or

   c. Addressing the risk requires corporate changes (e.g., changes to corporate policies); or

   d. Grievances from stakeholders have been received to which the Entity FoFo cannot impartially and/or effectively respond.

Our Family of Companies

Guidelines for Managing Expressions of Dissatisfaction & Threats from Third Parties With Whom The FoC Contracts With

1. If you receive either a verbal or written (hard-copy or electronic) expression of dissatisfaction from a Third Party with whom the FoC Contracts with
   - Provide details of the expression of dissatisfaction to both your Supervisor and Manager & GRC
   - Work with your Supervisor or Manager to research & provide a response to the expression of dissatisfaction
   - Provide a copy of your response to GRC
2. If you receive either a verbal or written (hard-copy or electronic) threat from a Third-Party with whom the FoC Contracts with in terms of but not limited – contract termination for cause, the levying to penalties/fees, the intent to exercise a right such as filing a dispute, invoking arbitration, considering possible legal action etc.
   - Provide details of the threat to your Supervisor or Manager, your Business Unit Lead and GRC
   - Do not engage with them directly unless in the normal course of business. Await direction from GRC in collaboration with your Supervisor or Supervisor or Manager and Business Unit Lead in terms of any response to the Third-Party specific to the threat
   - Continue to refer any follow-up communications from the Third Party related to the threat to your Manager, your Business Unit Lead and GRC until advised to the contrary
3. If you receive either a verbal or written (hard-copy or electronic) communication from Counsel representing a Third-Party with whom the FoC Contracts with (such communication may or may not include a threat of legal action)
   - At your earliest convenience provide details of the communication to both GRC and your Business Unit Lead (with a courtesy notification to your Supervisor or Manager)
   - Do not respond to Counsel and/or the Third-Party (any communication will come from GRC and/or your Business Unit Lead)
   - Refer any follow-up communications from Counsel and/or the Third-Party related to the communication from Counsel directly to GRC and your Business Unit Lead. Do not engage with Counsel. Only engage with the Third-Party to the extent that is necessary to continue normal business

operations.

- As a best practice retain ALL documentation related to the Third-Party (pending the possible imposition of a formal Legal Hold)

These guidelines do not apply to client or employee specific complaints, grievances etc. You should continue to follow existing processes in that regard.

Any questions or if in doubt as to what you should do, please contact GRC at compliance@catalight.org.

Our Family of Companies

Guidelines for Reputation Management Monitoring and Escalation

Reputation risk is any threat to our company's good name. This can happen when our company's character or ethics are called into question. Be vigilant about client/customer service mishaps and report:

1. Client/customer complaints of any kind
2. Issues or concerns with service line or clinicians/staff
3. Disparaging comments or confidential information from an employee
4. Disparaging comments from an external FoC event attendee, vendor or donor
5. A false or mistaken remark about another affiliate, entity, employee or FoC service line (this includes Social Media as well as both Verbal & Written communication mediums)

REVIEW	COMPANY	GENERAL RESPONSE	LEVEL 1	LEVEL 2	LEVEL 3
General dissatisfaction	All	Apology; Refer to Customer Service	Marcom, Customer Service; leader*	Quality/GRC	Population Health Oversight
Issues with service line or clinician	BHPN ESNorCal ESH myBrightlink	Apology; Refer to Customer Service or Quality	Marcom; leader*	Quality/GRC	Population Health Oversight or Clinical Ops
Disparaging or confidential employee comments	All	Removal of comment OR note follow-up by email	Employee's Supervisor; leader*	Quality/GRC	P&P
Disparaging comments from external partners	All	Removal of comment OR note follow-up by email	Quality/GRC; leader*	Vendor partner(s) in FoC	P&P
False/mistaken remarks of affiliate, service, etc.	BHPN ESNorCal ESH myBrightlink	Address with correction and supporting resource (if possible)	Marcom; leader*	Skip to →	Population Health Oversight, P&P, Clinical Ops

Our Family of Companies

Guidelines for Reporting Information Privacy-Security & Cyber Security Threats

The Information & Cyber Security Reporting Guideline provides a series of channels through which incidents can be reported, escalated, and administratively reviewed to ensure the FoC's information assets and/or infrastructure are protected. The Office of Information Security and the Office of Governance, Risk & Compliance (GRC) will be the primary responders to the incidents. Other departments will assist as the need arises.

* AFTER NOTIFYING THE OFFICE OF INFORMATION SECURITY AND THE OFFICE OF GRC, IT IS ESSENTIAL TO FOLLOW THE INSTRUCTIONS OF THE INCIDENT RESPONSE TEAM.

Examples of what type of incidents should be reported appear below:

- Any suspected phishing or other social engineering attempts
- Any suspected hacking or intrusion attempts
- Suspicion of a password compromise
- Harassment by e-mail
- Violation of any information privacy security or technology policy

Legal and Other Obligations

1. Determine if the threat requires the involvement of legal counsel (refer to GRC for guidance)

2. Develop an information privacy-security or cyber incident response plan (IRP) as outlined in the Business Continuity Plan. The IRP should be based on:
   a. the nature of its business or other activities;
   b. the data it collects and maintains; and
   c. the locations where it operates and its employees and customers or clients are located.

3. Developing and maintaining an IRP may help the FoC:
   a. prepare to respond more rapidly and effectively to cyber events;
   b. lessen the effects of a data breach or other information privacy-security incident; and
   c. demonstrate that the FoC has taken reasonable steps to maintain adequate cybersecurity practices if an incident results in litigation or enforcement action.

4. Is the FoC subject to laws or regulations that require notification to affected individuals, regulators, or others if a data breach of personal information occurs and, if so, determine:
   a. required timelines for notifications;

b. the populations for which the FoC stores personal information and how the FoC intends to contact them;
c. exceptions to notification obligations that may apply to the FoC, such as whether data is encrypted or a harm threshold apply;
d. whether the FoC plans to use external service providers to notify affected individuals; and
e. how and when any vendors or other third parties with access to the FoC's IT systems, network, or data, or that handle personal information on the FoC's behalf, intend to notify the FoC if an information privacy-security incident occurs in their environments.

5. Has the FoC entered into contracts with customers, clients, or other business partners that obligate it to maintain an IRP or provide data breach or cyber incident notification.

For more details on identifying legal and other obligations when developing and maintaining an IRP and providing data breach notification across jurisdictions, see the Business Continuity Plan and Breach Notification Standard.