Johnson & Johnson

September 07, 2018

Dear Johnson & Johnson Leaders:

At Johnson & Johnson, we work to create an environment in which every employee throughout our Family of Companies understands his or her responsibility to report a potentially serious violation of our policies or the law, or where there are other substantial risks that could jeopardize our reputation. With this annual message, here's a quick reminder of the seven key categories of issues that are required to be escalated to Steve Bariahtaris, Vice President, Corporate Internal Audit using either the Credo Hotline [Link here] or directly.

Additionally, all privacy violation or data breach incidents should be escalated to the J&J Global Service Desk (this reporting can be done by phone (1- 855-561-IRIS (4747)), or via the Case Management System using the "IRIS" Self-Service Portal. A link to the full escalation policy is here (click here to see the translated versions of the policy). Please ensure this reminder is shared throughout your organization.

In summary, each employee should escalate any of the following issues if they are believed to exist:

- Expense Report or Global Travel Meetings and Expense policy violations in excess of USD 1,000
- Theft, fraud, defalcations, or other significant loss of Company funds in excess of USD 1,000
- Violations of law; or violations of a critical contractual clause by a third party that could result in a significant financial loss to J&J (which loss must exceed $1,000).
- Actual or potential violations of Johnson & Johnson policies on Financial Reporting, Government Contract Compliance, Health Care Compliance, International Health Care Business Integrity, the Johnson & Johnson Code of Business Conduct, or the Code of Business Conduct and Ethics for members of the Board of Directors and Executive officers
- Any actual or potential non-compliance with our U.S. government contracts or pricing obligations (regardless of severity or apparent financial impact)
- Any allegations of misconduct by a senior leadership team member of a business unit, operating company or support function
- Potentially substantial risks to the reputation of Johnson & Johnson or one of its business units that is not already reported under Worldwide Quality, Security or EHS procedures
- Data breach or privacy incidents (such incidents are to be escalated irrespective of the value of any hardware/equipment that may have been the repository of such data)

Thank you for your help in ensuring this important communication is shared throughout your organizations.

John Crisan
Chief Compliance Officer
jcrisan@its.jnj.com

Steve Bariahtaris
Vice President, Corporate Internal Audit
sbariah1@its.jnj.com

Johnson & Johnson

ESCALATION PROCEDURE

1. Introduction

This document sets out the Johnson & Johnson Escalation Procedure. Timely escalation in accordance with this policy is critical in view of obligations the Company may have to disclose events reportable under this policy to government bodies, the heightened emphasis on internal controls to assure compliance with laws and regulations, the serious potential legal and reputational consequences of significant compliance failures and the need to appropriately investigate, analyze and remediate control issues, as appropriate. Failure to do so may expose the Company or its employees to potential legal sanctions.

2. Scope of Escalation Procedure

Those items identified in Section 3 below should be escalated and reported as required under this Escalation Procedure. Items should be escalated regardless of whether uncovered as a result of self-detection through financial controls, testing and/or monitoring, or whether identified through the receipt of signed or anonymous letters or calls, employee hotline calls or reporting by employees directly to the Law Department, Internal Audit, line management or other corporate staff.

Those items that are out of scope of this policy, or that are also covered by other procedures, are set out in Sections 5 & 6 below.

3. Escalation Procedure: When Corporate Internal Audit Must Be Notified

It is critical that the Vice President, Corporate Internal Audit, be notified within **three (3) business days** (either verbally or in writing, including by e-mail), as soon as any of the following conditions are believed to exist, even though full details might not yet be available:

a. There is an actual or potential violation of the Johnson & Johnson Expense Reporting Policy or the Johnson & Johnson Global Travel Meetings and Expenses policy and the amount in question exceeds USD 1,000 or involves a national, state or local government employee.

b. An actual or suspected theft, fraud or defalcation occurs, or there is any other situation that potentially involves a significant loss of Company funds, in any case that may exceed USD 1,000 (escalation is required regardless of whether the matter may be covered by insurance).

c. There is an actual or potential violation of any of the following policies that could result in an employee, including a temporary employee, being terminated or suspended:
   - Johnson & Johnson Financial Reporting Procedures

- Johnson & Johnson Government Contract Compliance Guidelines (escalated in accordance with Appendix B)
- Johnson & Johnson Health Care Compliance Guidance Policies
- Johnson & Johnson International Health Care Business Integrity Guide
- Johnson & Johnson Code of Business Conduct
- Johnson & Johnson Code of Business Conduct and Ethics for members of the Board of Directors and Executive officers.

For clarity, the USD 1,000 threshold referred to in other sections of this policy does not apply to violations referenced in this sub-section (c).

d. There is an actual or potential violation of law (including instances when any Johnson & Johnson company is informed that a government investigation has been started or is ongoing) by a Johnson & Johnson company, employee or agent that could result in a fine, monetary penalty or administrative sanction (regardless of the amount), criminal prosecution of the Company or its employees, or other legal or regulatory consequence. Actual or potential violations of the FCPA or any other anti-corruption law must ALWAYS be reported.

e. Data breach or privacy incidents, escalated as specified in Section 4 below. Such incidents should be escalated irrespective of the value of any hardware/equipment that may have been the repository of such data.

f. A third party has or potentially has violated a critical contractual clause when violation of such a clause could result in a significant financial loss to Johnson & Johnson.

g. Any allegations of misconduct by a member of the senior leadership team of a business unit, operating company, or support function (or equivalent level position).

h. There is a potentially substantial risk to the reputation of Johnson & Johnson or one of its business units that is not already required to be reported under Worldwide Quality, Worldwide Security or EHS procedures.

Investigative work should not be started before this notification, except as necessary to verify whether the allegation meets the criteria above. Moreover, any locally initiated investigations do not exonerate management of our companies to escalate reportable events under this policy. In the event law enforcement authorities issue search warrants or take an employee in custody, Worldwide Security and the Law Department should both be notified to coordinate the appropriate response.

Notification should include at least a preliminary description of the event(s) that occurred (based on the details available at the time of the notification), when the event(s) occurred, how the issue was originally detected, the potential dollar quantification of the issue and the name and title of person(s) having relevant information related to the occurrence.

Appendix A to this Escalation Procedure sets forth illustrative examples of items that should and should not be escalated under this Escalation Procedure.

4. Separate Escalation Procedure: For Privacy and Data Breach Matters.

Regardless of how an incident is detected or what data may be involved, it is the responsibility of each Johnson & Johnson employee or contractor and/or external service provider to report any privacy or data incident (including any potential breach of privacy policies, or any event that may potentially affect or has affected the confidentiality, integrity or availability of Personal Data irrespective of its format (paper, electronic, or otherwise)). Although within scope of this escalation procedure, **reporting should be to the J&J Global Service Desk (this reporting can be done by phone (1- 855-561-IRIS (4747)), or via the Case Management System using the "IRIS" Self-Service Portal (using chat or by submitting an Incident Ticket).**

The J&J Data Breach Response Team oversees, reviews and handles all escalations of privacy/data incidents as a sub-committee of the J&J Triage Committee. The J&J Data Breach Response Team will promptly notify the J&J Triage Committee when any of the following criteria are met with respect to a data or privacy incident: reporting is envisaged to regulator or data subjects; fines or enforcement; potential media exposure; or reputational damage. All other data or privacy incident escalations shall be notified to the J&J Triage Committee on no less than a quarterly basis by the J&J Data Breach Response Team.

5. Out of Scope of Escalation Procedure: HR Matters.

The Human Resources community is responsible for addressing allegations of harassment and discrimination. Those types of allegations are excluded from the scope of this Escalation Procedure unless also related to any of the items specified in Section 3 or Section 4 above. Also excluded are allegations that arise in the context of lawsuits brought by or against Johnson & Johnson or any of its operating companies unless related to any conditions mentioned as reportable hereunder.

6. Overlap With Other Escalation Procedures.

Other departments such as Worldwide Quality, EHS and Corporate Security may have in place escalation procedures that require notification to those offices when certain events occur. This policy is not intended to modify any of those processes. However, if there is an appearance, indication or evidence that those reportable events would fall within scope of Section 3 or Section 4 above, then such events must also be reported under this Escalation Procedure.

7. Repository for Escalated Issues.

The Vice President, Corporate Internal Audit, will serve as the focal point for receiving reports.

8. Conducting the Investigation

All cases will be handled consistent with the Triage Committee process. Depending on the facts and circumstances of any issues reported to Corporate Internal Audit, the Triage Committee will review and determine which corporate organization will take the lead in conducting the investigation. The Triage Committee consists of the Chief Compliance Officer; the Vice President, Corporate Internal Audit; representatives from the Law Department; and, on an *ad hoc* basis, representatives from Worldwide Security and Human Resources.

Once a matter is escalated to Corporate Internal Audit, the Operating Company and its management concerned should not conduct any investigative steps, and should not contact anyone else about the matter unless advised to do so by Corporate Internal Audit, the Law Department, or Health Care Compliance & Privacy.

With respect to those issues reported to it that do not require Triage Committee consideration, the Triage Committee will determine whether to delegate responsibility for the investigation to the Operating Company or a third party. Operating Companies to whom investigative responsibility has been delegated are responsible for timely investigation, adequate documentation, and resolution. Corporate Internal Audit and/or the Law Department may assist or advise the Operating Company to facilitate the investigation. Final results of investigations conducted by Operating Companies must be promptly reported to Corporate Internal Audit and, where appropriate, input into the applicable case management system. Operating Companies are also responsible for inputting corrective actions into the database which is used to track corrective actions.

9. Questions

If you have any questions, please contact John Crisan or Steve Bariahtaris.

John Crisan
Chief Compliance Officer
jcrisan@its.jnj.com

Steve Bariahtaris
Vice President,
Corporate Internal Audit
Sbariah@its.jnj.com

APPENDIX A

Examples of When CIA should be notified:

- Any allegation that an employee falsified or altered a document or record required to be kept under applicable government laws and regulations and/or J&J policies
- Any allegation of employee misconduct during the course of a government inquiry or investigation, such as a knowing or intentional misrepresentation to a government official or investigator, or inappropriate destruction of documents
- Fraudulent (e.g., fake or altered) receipts were submitted to an expense report if the aggregate amount involved exceeds USD 1,000. However, if the aggregate amount does not exceed USD 1,000, reporting to CIA is still mandatory when there is a suspicion or indication that it could relate to a violation of FCPA or other anti–corruption laws.
- Allegations of improper payments to government officials or other breaches of the FCPA or anti–corruption laws
- Allegations of payments to health care professionals that are not in accordance with Johnson & Johnson policies (irrespective of the amount involved)
- Payments were made or other items of value were given to a third party (e.g., vendor, customer) that are inappropriate because prohibited by a Johnson & Johnson policy or because payment was not in exchange for value received from the third party
- A conflict of interest between an employee and a vendor or customer is alleged and was not previously investigated, approved and communicated in accordance with the Code of Business Conduct
- Financial statements that have been falsified as a result of entries that appear to be deliberately erroneous
- Allegations of non-compliance with antitrust or competition laws
- Allegations regarding misappropriation of confidential information or trade secrets
- Company assets were given to Johnson & Johnson employees or any other person for non-business reasons, e.g., an employee gives a vendor USD 500 in gift checks
- Information submitted to the government (verbally or in writing) was inaccurate, including but not limited to, pricing, government calculations, business practices, certifications, disclosures or responses to audits/inquiries
- A failure to abide by or meet the requirements of a government contract or pricing program

Examples of When Corporate Internal Audit should not be notified:

- An employee fails to attach receipts for items over USD 25.00, but it has been demonstrated that the underlying transactions do not violate any Johnson & Johnson policies. This should be addressed at the Operating Company level.
- Potential violations that involve harassment, physical altercations, discrimination and similar violations. These matters should be addressed by the HR organization with Law Department involvement as necessary.
- Potential violations of Johnson & Johnson policies that would clearly not result in an employee being terminated or suspended. These matters should be addressed at the Operating Company level.

APPENDIX B

U.S. Government Contract and Pricing Supplement to Escalation Procedure

Distribution

This Supplement should be read by all members of a Johnson & Johnson organization who have direct or indirect responsibility for selling to or contracting with the U.S. Federal Government or whose products may be reimbursed by U.S. Federal government entities.

Background

Johnson & Johnson employees are required to comply with all applicable federal, state, and local laws, regulations, contract terms and conditions, and related Johnson & Johnson policies governing our business operation, and to report any prohibited or unlawful acts of which they are aware. The Johnson & Johnson Operating Companies are each responsible for carefully monitoring compliance, and there is an established escalation procedure to ensure appropriate investigation and resolution of issues as they arise.

To this end, the world-wide Escalation Procedure establishes the protocol for reporting of any potentially serious violation of law that could result in a significant fine or other substantial legal consequences. It requires that the Vice President, Corporate Internal Audit (CIA), or their designee, be notified within three (3) business days either verbally or in writing, including by e-mail, if certain violations are believed to exist. Notice to CIA is required in this timeframe even when full details, including validation or financial impact, are not yet available. This is necessary to assure that the outcome of any investigation or determination of compliance is not compromised by the manner in which such matters are reviewed. Personnel are permitted to inform their management or a law department representative of potential concerns prior to notifying CIA, so long as the matter is appropriately reported to CIA within three (3) business days of the matter initially being identified. Stated differently, the three day clock starts to run when the matter is initially raised, *not* after it has been reported to an individual's supervisor. Corporate Internal Audit acts as a central repository for all reported matters and monitors the timely investigation and resolution of these potential violations. Depending on the facts and circumstances of any issues reported to Corporate Internal Audit, the Triage Committee will convene and determine which organization (HCC/GCC/Law Department/CIA or Operating Company) will take the lead in conducting the investigation.

GCC Supplement to the Escalation Procedure for Federal Contractors

The purpose of this memo is to remind individuals that since December 2008, Johnson & Johnson affiliates who contract with the United States Federal Government ("Federal Government") have been subject to an additional requirement known as the Mandatory Disclosure Rule. This rule requires companies that contract with or sell to the Federal Government to timely disclose "credible evidence" to the government of certain violations of criminal law (involving fraud, conflict of interest, bribery or gratuity violations with government employees or officials), violations of the civil False Claims Act, or significant overpayments in connection with the award, performance, or closeout of the government contract. Separately, under FAR 52.222-50 (Ending Trafficking in Persons) (March 2015) (the "Human Trafficking Rule"), companies that contract with or sell to the Federal Government are also required to immediately disclose "credible information" to the government relating to allegations of trafficking in persons by the Company, any employee, subcontractor, subcontractor employee or agent. Failure to make a timely disclosure subjects the Johnson & Johnson Company, as well as any principals of the Company that had such knowledge and failed to act, to suspension or debarment from Government contracting. The

Company also may be subjected to additional fines and penalties. The Mandatory Disclosure rule and Human Trafficking Rules are two of several that have been implemented recently to provide the Federal Government with more information about potential contractors towards the goal of assuring that the Government is spending taxpayers' money responsibly.

Adherence with our obligations under the Mandatory Disclosure Rule and the Human Trafficking Rule, as well as other transparency obligations, is facilitated through the GCC Supplement to the Escalation Procedure. The GCC Supplement adds two requirements to the Escalation Procedure: (1) it identifies additional types of potentially non-compliant activity that must be reported, and (2) it establishes a different threshold for reporting situations that have the potential to impact GCC compliance. These additional escalation obligations are designed to ensure that all circumstances that *may* equate to a non-compliance with a Government contracting or pricing obligation are fully reviewed and the proper disposition is made and documented, even for those situations that are determined not to warrant disclosure under the Mandatory Disclosure Rule. Further, these escalation procedures are designed to allow for an immediate disclosure of "credible information" concerning an alleged violation of the Human Trafficking Rule. Your cooperation with this procedure further enables our collective compliance.

Reports

Johnson & Johnson has many channels available to receive reports of possible violations, including: line management, compliance professionals throughout the organization, the General Counsel and members of the Johnson & Johnson Law Department, the Compliance "hotline," and Corporate Internal Audit. Any of the above who receive reports covered by this policy are required to timely notify Corporate Internal Audit or so that the matter can be tracked and a thorough review conducted.

When Corporate Internal Audit must be notified

The Vice President, Corporate Internal Audit ("CIA") must be notified (1) as soon as, and in no event later than three (3) business days after, any of certain conditions are believed to exist, even though full details may not yet be available and the impact to Government contract compliance is not yet determined; and (2) immediately of any credible information suggesting that a violation of the Human Trafficking Rule has occurred. This notification can take place orally or in writing, including via e-mail. It is permissible to contact and discuss the relevant circumstances with a designated subject matter expert in the Law Department or a designated Compliance contact prior to notifying CIA, so long as the notice to CIA occurs within the required three (3) business days. With respect to reports concerning the Human Trafficking Rule, it is permissible to contact and discuss the relevant circumstances with a designated subject matter expert in the Law Department or a designated Compliance contact concurrent to reporting the information to CIA. The designated legal subject matter experts for government contract and pricing matters are (as of the date of this policy) Stephanie Gilson, Jessica Empestan, and Perry Knight in the Regulatory Law Group. An individual is permitted to discuss a potential non-compliance with their supervisor prior to reporting the matter to CIA or the Law Department, so long as the other requirements stated here are met. In this circumstance, the supervisor shares responsibility for assuring that the potential non- compliance is properly and timely escalated. Except as provided for here, information about a potential non-compliance should not be shared with anyone other than CIA or the appropriate subject matter experts in the Law Department, nor should any investigative or other work be performed on the issue until further direction is received from CIA or the Law Department.

Triggering Events

While it is not possible to list here each and every possible noncompliance relevant to government contracting and pricing that must be reported, we have endeavored to identify certain categories and specific exa[illegible] are subject to the

Escalation Procedure. Please note that potential violations must be reported whether they involve the Company, its officers, directors, managers, employees, agents, vendors, subcontractors, partners or others with whom it does business. While the Escalation Procedure generally requires the reporter to make a reasonable determination of severity in order to identify those issues which should be reported to CIA versus handled internally, all actual or potential noncompliances must be reported—regardless of severity or apparent financial impact—if it might impact compliance with our government contracts or pricing obligations. Thus, it is anticipated that in some, if not many instances, a simple mistake, a human error, or an immaterial non-compliance with a commercial contract or practice will be escalated because of its potential impact on government compliance. Consider also that the timely identification and reporting of even these situations with immaterial impact enables Johnson & Johnson to demonstrate that it has an effective compliance program in place and to rectify problems prior to there being a material financial impact. Notwithstanding the guidelines above, any credible information concerning a potential violation of the Human Trafficking Rule must be immediately reported to CIA.

Specifically, individuals must timely report to CIA any information related to:

1. An actual or potential violation of the Johnson & Johnson Expense Reporting Policy involving a federal, state, or local government employee.
2. An actual theft, fraud, or defalcation occurs or there is a reasonable basis to suspect that a theft, fraud or defalcation has occurred that, in either case, may relate to a government contract.
3. An actual or potential violation of the Johnson & Johnson Government Contract Compliance Guidelines.
4. A false statement was made to the government, whether orally or in writing, or there was a failure to timely disclose required information to the government.
5. A failure to abide by the terms of a government contract or pricing program, whether it results from failure to timely and accurately disclose pricing, failure to charge the agreed upon price or pay appropriate rebates, failure to perform required processes or tests, failure to deliver products that conform to contract requirements, or failure to adhere to country of origin requirements.
6. A third party performing services relating to government pricing or contracting compliance has or potentially has violated a critical contractual clause, including an actual or potential violation of the Human Trafficking Rule.

Accordingly, items that should be reported to CIA include, but are not limited to, the following. Please note that this list is not exhaustive, and when in doubt, report the information so that the appropriate experts can perform a thorough review.

- An error is discovered in a previously submitted government pricing calculation. Some causes for this may include, but are not limited to, an error in the formula used, use of incomplete data, or miscategorization of a payment, inaccurate or incomplete commercial sales data
- Country of manufacture for a product was changed resulting in a different Country of Origin, without disclosure to affected government purchasers (i.e. Trade Agreements Act/Buy American Act violations)
- Violations of the Price Reductions clause in FSS contracts, either due to failure to timely disclose, incomplete disclosure, or failure to adjust price
- Defective Pricing resulting from failure to adequately disclose commercial sales practices
- Invoices issued to government payors reflecting an incorrect payment amount
- System issues that have broad implications & government transactions are processed in the same system
- Misstatements made in connection with c ontract negotiations with or proposal submissions to the government
- Falsification or unauthorized destruction of Company books & records

- Consulting agreements with government employees or officials entered into without written evidence of permission from designated Government ethics representatives.
- Instances of gratuities (including meals) given to Government employees or officials in excess of permissible limits or circumstances
- Instances of grants made to Government or Government-affiliated entities without written evidence of internal and government approvals
- Credible information suggesting that a Company has engaged in violation of the Human Trafficking Policy, such as charging employee's recruitment fees, or failing to provide employment contracts or work documents where required by law

If you have any questions related to the Mandatory Disclosure Rule, please contact the Johnson & Johnson Law Department (as of the date of this policy, contact Stephanie Gilson, Danielle Berti, Perry Knight). If you have any questions related to the Escalation Procedure, please contact John Crisan or Steve Bariahtaris.

Document Approvals
Approved Date: 16 Sep 2018

Approval Task Verdict: Approve	John Crisan, (jcrisan@its.jnj.com) Business Approval 06-Sep-2018 13:04:06 GMT+0000

Approval Task Verdict: Approve	Steven Bariahtaris, (SBariah1@its.jnj.com) Author Approval 16-Sep-2018 22:33:44 GMT+0000