As part of HSSE information sharing, please note that the updated **Security Breaches Procedure** has been approved by HSSE Implementation Committee.

The updated procedure can be accessed thru the following link:

Security Breaches Procedure

All Directorates, Groups and Teams are requested to ensure that this information is shared among all the employees including Contractors and Sub Contractors for necessary implementation.

Regards,

Security Team (Support Services)

Security Breaches Procedure Document Number:

Document Author:	Manager (Security)	**Document Coordinator:**	TL Security (SS)
Approved by:	KOC HSSE Implementation Committee		
Authorized by:	KOC HSSE Implementation Committee		
Original Issue Date:	March 20, 2011	**Document Control Tier:**	Tier 3
Revision/Review Date:	March 09, 2014	**Next Review Date:**	March 10, 2017

1.0 Purpose / Scope

The procedure describes the process and responsibilities for internal reporting of Security Breaches which occurs in KOC operational areas or related to KOC activities.

2.1 **Definitions**

2.1 Security Breaches - Security breaches / incidents refers to Internal / External acts that bypass security policies, practices or procedures such as the disclosure of classified information (closed information not available to all KOC employees), access to protected assets without authorization, theft including Vandalism, arson, Bomb and Firearms incidents.

2.2 Restricted area – A restricted area is that area, in which KOC exercises control over all movements, operations & maintenance activities i.e. the area within the fenced boundaries or open space where KOC has direct or indirect control for operational reasons.

2.3 Confidential information (classified information) - A restricted document / information where access is available only to select few within KOC and to be distributed to identified personnel on the written authority of KOC senior management personnel.

2.4 Highly Confidential information (highly classified information) - A restricted document / information available to select few within KOC.

Documents are classified as restricted or highly classified when unauthorized disclosure would:

- Cause harm to the people or Govt. of Kuwait.
- Cause harm to KOC personnel or subsidiary.
- Be in contradiction to applicable laws, regulations policies or codes of KOC.
- Cause serious embarrassment to any individual, KOC, or the Govt. Authority that had provided information to KOC.
- Give an unfair advantage to any individual or entity.

Table 1: Security Breaches Categorization – Description

Minor	Moderate	Major
Theft of KOC or individual property inside KOC Facilities.	---	Illegal detentions, kidnaps or unauthorized occupation of Company property.
Theft or any kind of violent criminal acts, minor vandalism or damage to Company property inside KOC Facilities and controlled area (loss not exceeding KD. 500).	Theft or any kind of violent criminal acts, vandalism or damage to Company property inside KOC Facilities / controlled areas (loss exceeding KD. 500).	Act of deliberate vandalism causing significant damage to Company property and Oil production facilities resulting in ceasing complete or partial production.
Unauthorized entry to company non-public areas (e.g. offices)	Unauthorized entry to Company Vital installations and restricted areas (e.g. GC's, BS's, Manifolds & Valve Stations on Transit Lines)	---
Loss of company owned, non-public information or documents in any medium that may have an adverse impact on KOC commercial confidentiality or reputation. For example; routine internal Memos and letters; administration, training or support matters.	Loss of any company owned, nonpublic information or documents in any medium that are marked as 'Confidential', or 'Commercial-inConfidence' or have a privacy marking, that may have an adverse impact on KOC commercial confidentiality or reputation. For example; Oil exploration surveys or plans or production informations, nonpublic contracts information; personal files, documents, databases. Also any attempt at unauthorized access to KOC IT network or individual, workstation whether or not successful.	Loss of any company owned, non-public information or documents in any medium that are marked as 'Secret', or 'Highly Sensitive Commercial-inConfidence' that may have any major adverse impact on KOC production, commercial confidentiality or loss of reputation. For example; future oil exploration policies, plans or production information, tender evaluation and financial contract information; disciplinary matter personal and medical files, documents and databases. Also any intrusion to the KOC IT network or an individual workstation whether or not information is known to be transferred, lost or network is disrupted.

---	---	Terrorist, insurgent or riotous attacks against Company personnel or property.
---	---	Bomb, incendiary or firearm incidents, including threats / hoaxes or any possible connected suspicious activity taking place within KOC controlled areas & premises.

Security breaches not falling in any of the categories mentioned in the above Table and in case has occurred in the contractor assigned sites even if within KOC premises, will be considered as a Miscellaneous breach and recorded as such in the system. Although all security related breaches and calls will be addressed and responded to, only breaches taking place within direct KOC's controlled facilities and operational areas are recorded. Hence, Security Breaches taking place in Ahmadi's township residential area (ie house theft, sabotage, etc) or outside KOC's controlled facilities and operational areas On / Off duty hours to be reported as Miscellaneous Breaches, and will not be considered recordable. However, with reference to the section 3.4, Area Security Team has the right to verify the details, confirm category during its approval stage.

3.0 Key Responsibilities

The following are defined roles and responsibilities for the implementation and maintenance of the KOC Security Breaches Reporting.

3.1 Observer

Observer of the incident can be a company employee, contractor employee or a visitor. The observer is responsible for immediate reporting of the breach to KOC's Emergency Control Center (160).

3.2 KOC Emergency Control Center (160)

Receiving the call from the observer and informing / confirming the Controlling Team about the incident/Security breach.

Coordinate with concerned Area Security Team (Ahmadi, S&EK, North Kuwait and West Kuwait), Asset HSE, Ministry of Interior (Operations Center) (MOI), Oil & Vital Installations Protection Department (O&VIPD), HSE D**irectorate**, Ambulance (if required),,,etc, whenever

required to respond properly to the Security Breach. Log all activities in Fire Incident Management System (FIMS).

3.3 Controlling Team

Responsible to verify that breach has been reported to ECC (160). Take immediate remedial action to minimize and control the loss associated with the breach with Area Security Team. Responsible for timely internal reporting of the security breach through the use of Security Breaches reporting mechanism (HSE Live). Lead / participate in related Security Breaches Investigation exercise to identify Root Cause, gaps and recommendations and responsible to take appropriate actions to close these gaps. Provide regular reports to Area Security Team and a copy to Security Team Support Services on the action status of identified recommendations.

3.4 Area Security Team

Respond to Security Breaches calls received from ECC. Coordinate with Controlling Team & ECC for the required controlling measures and resources. Review the Security Breach report issued by the Controlling Team, verify the details, confirm category and approve it. Participate in related Security Breaches investigations to identify Root Cause, Gaps and recommendations. If required, Area Security Team shall seek the assistance of State Security Agencies.

3.5 Security Team (Support Services)

Performs regular review of the Security Procedure as per the specified review date. Analyze Security Breaches data and communicate the same to KOC's Management. Receive regular reports from Controlling Team(s) on identified gaps & recommendations action plan and progress.

4.0 Procedure

- The observer (KOC/Contractor employee or visitor) informs KOC ECC (160).
- ECC alerts the Area Security Team who goes out to check the area of the incident to assess the situation and reports back to ECC for assistance from Medical, HSE Asset Team and State Security Agencies if the situation warrants it.
- ECC in turn places calls to all required Teams to assist in containing the situation and rendering medical assistance to those in need and to the Controlling Team of where the incident has occurred.
- Responding Teams will determine categorization of incident and subsequent course of action.

- The Controlling Team will post details of incident within 24 hrs. of the incident.
- An investigation committee comprising of members from the Controlling Team, Asset HSE, Area Security and any other required discipline as identified in clause 4.4will be instituted to carryout investigations, and come up with recommendations to prevent similar incidents occurring in future.
- If the security breach is that which requires state security agency involvement it will be handed over to them to carry out the required investigations.
- Security breach incident that obtain Management clearance only will be posted as "Lessons Learnt" for general viewing.

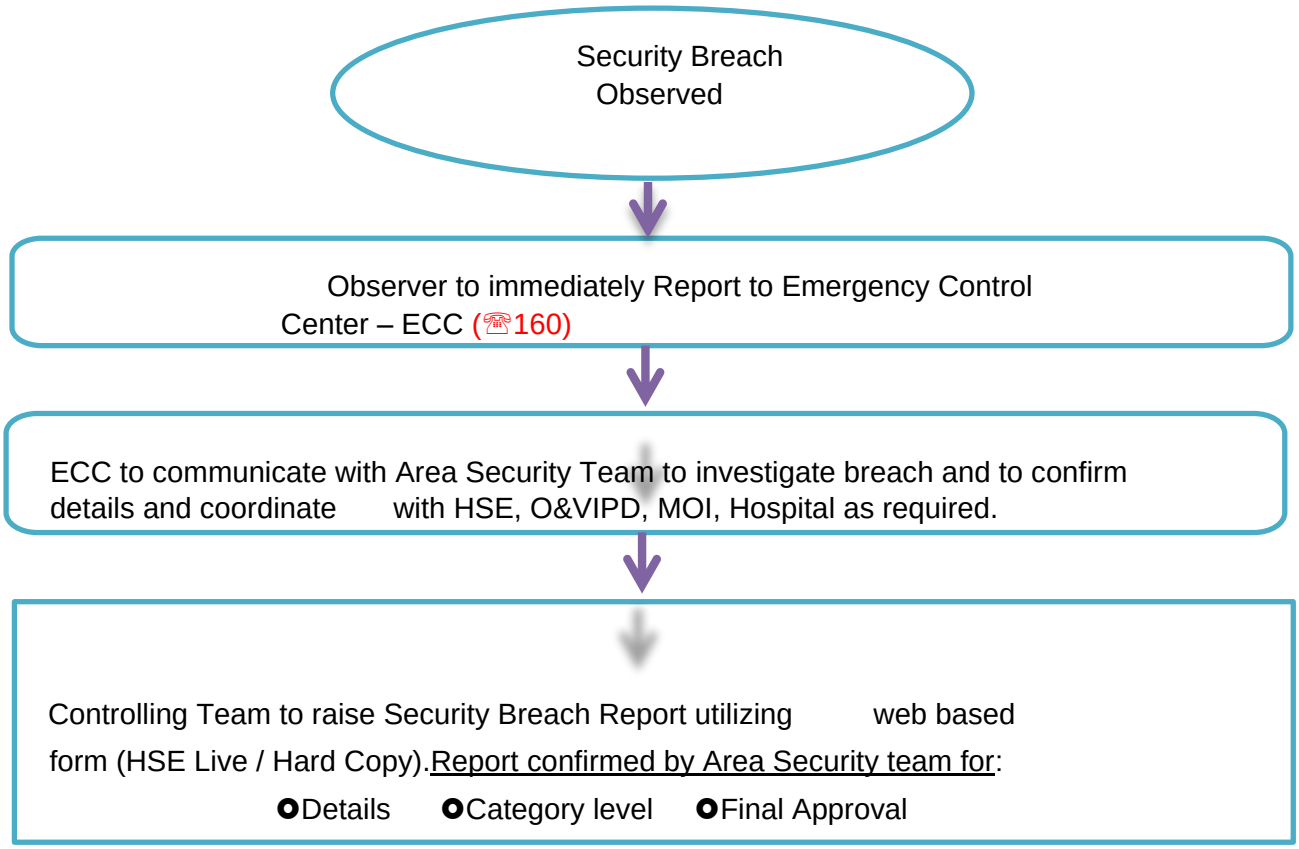
Time line of reporting:

All security breaches are to be reported through HSE Live within 24 hours of incident occurrence or on the next immediate working day. However, it shall be further updated in HSE Live by the Originator / Controlling Team Leader based on the preliminary investigation carried out by responding Security Officers.

4.1 Breaches Reporting

FLOW Diagram

Phase – I (Breaches Reporting)



Phase – II (Breaches Investigation)

Major Security Breach:

Investigation Committee formed by KPC CEO & chaired by DCEO from another K-Company comprising of at least seven (7) members from following departments / agency:

- Outside Directorate & HSE Group or Team / Security Group representatives.
- KPC & its subsidiaries
- Scientific / Technical / Academic Gov't. Agency & Legal Agency.

Minor Security Breach:

Local Investigation – To be investigated by controlling Team Leader & respective area Chief Security Officer / Security Officer.

Moderate Security Breach:

Investigation by Committee within Directorate managing the activity where incident occurred. The committee to be headed by Controlling Team Leader with Area Security Team Leader as a member.

Identify shortfalls, gaps, accountability and develop recommendations to be communicated to all concerned.

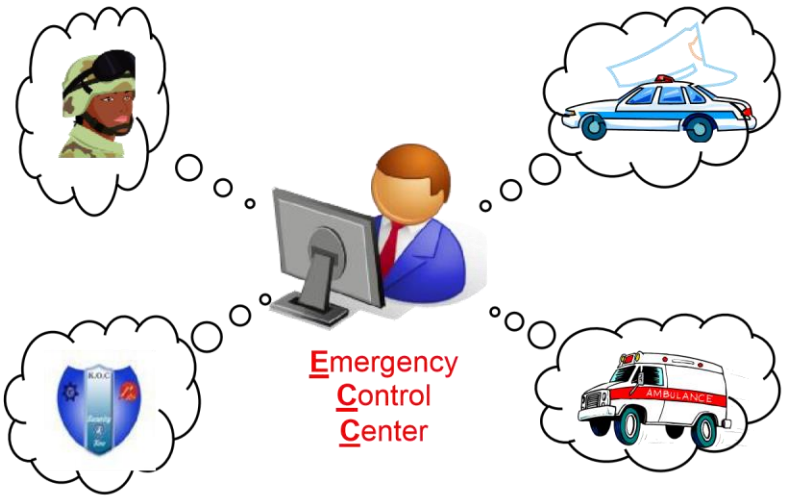
Follow-up

Findings & recommendations to be forwarded to Controlling Team. Controlling Team to provide regular update on action item & recommendations to Area Security Team and copy to Security Team (SS).

Security Team (SS) submits regular reports to KOC Management to track the progress / completion of any recommended actions.

SECURITY BREACHES

Security Breaches Observed



Emergency Control Center

Primary Investigation

Data Base
(Security Team-SS)

Breach Investigation
(Investigate, Identify Gaps, Recommendations, Actions, Tracking & Completion)

Final Approval
(By Area Security Team)

HSE Live
(Originated by Controlling Team)

4.2 Security Breach Database

Data submitted through Security Breaches forms / HSE Live will be recorded in a central Security Breaches Database maintained by Security Team (SS). Access to the database will be controlled and serve as the official archive for incident data.

4.3 External Agency & Company Reporting

Summary of Security Breaches reporting and other required notifications to external agencies and interested parties outside of KOC *(such as KPC and / or the public)* shall be coordinated through Security Team (SS).

4.4 Initial Breach / Incident Investigation & Root Cause Analysis

The Chief Security Officer / Security Officer of the concerned Area Security Team and the Controlling Team Leader or his representative shall investigate Minor Security Incidents locally. Immediate & Root Causes as well as corrective actions are recorded in the Incident Investigation Report**.**

Moderate incidents require the establishment of an Investigation Committee within Directorate managing the activity where incident occurred. The committee shall be headed by Controlling Team Leader with Area Security Team Leader as a member.

Major incidents are investigated by Investigation Committee formed by KPC CEO & chaired by DCEO from another K-Company comprising of at least seven (7) members from following departments / agency:

- Outside of Directorate & HSE Group or Team / Security Group representatives.
- KPC & its subsidiaries
- Scientific / Technical / Academic Government Agency & Legal Agency.

Detailed Incident Investigation report and Root Causes and Recommendations are to be communicated to all concerned parties for action with a copy to Area Security Team, Security Team (SS) & Asset HSE / Directorate for follow-up.

4.5 Communicating Lessons Learned

Once breaches / incidents have been reported and investigated *(locally for minor breaches; or through an independent investigation committee for major / moderate breaches)*, as well as initial corrective and preventive action developed; then significant lessons learned from the

incident shall be communicated – both within KOC and other KPC organizations - as deemed appropriate.

4.5 Key Documents / Tools / References

- HSE Live
- C&MD's Revised KOC Security Policy Statement
- KPC CEO Directives on Investigation of Major Incidents
- KOC General Emergency Procedure
- KOC.GE.025 – KOC Crisis Management Plan
- KOC.GE.026 – KOC Corporate Emergency Response Plan

4.6 Abbreviations

- CEO – Chief Executive Officer
- DCEO – Deputy Chief Executive Officer
- KPC – Kuwait Petroleum Corporation
- KOC – Kuwait Oil Company
- HSE – Health, Safety and Environment
- KD – Kuwait Dinar
- TL – Team Leader
- SS – Support Services
- GC – Gathering Center
- BS – Booster Stations
- ECC – Emergency Control Center
- MOI – Ministry of Interior
- O&VIPD – Oil & Vital Installations Protection Department