MACD Information Confidentiality Practices

These practices address the management of confidential information (as defined in the IESO market rules) between MACD and IESO business units. The IESO market rule address management of confidential information outside the IESO Corporation. In addition to following the IESO market rules and the IESO Information Confidentiality Policy, Compliance Enforcement, MAU staff, and contractors are required to follow some additional rules surrounding confidential information management between MACD and IESO business units. The following applies to information regarding monitoring activities, investigations, adjudication, and litigation from either internal or external sources produced, in the possession of MACD in any form (eg. verbal or written, recorded, or electronic or otherwise) concerning either Ontario market participants or the IESO. This information will be referred to as "MACD information" in this procedure. This procedure applies to temporary or permanent MACD staff and any contract staff working for MACD. The following procedure uses the term "MACD staff" to mean MACD temporary or permanent staff and contractors.

Handling MACD Information

Market Participant Matters

For case assessment regarding Ontario market participants MACD may use IESO business units to aid in assessing information as subject matter experts for investigations for monitoring purposes. Regardless of the method of receipt or production of information it is not to be disclosed to other business units of the IESO other than on a need-to-know basis. When possible, information to support monitoring or investigative activities should be provided to IESO business units verbally. If written information is provided to the IESO business unit(s), once the required input is provided by the business unit, MACD is to request the IESO business unit(s) destroy the information and not to distribute it unless they seek your approval.

IESO Matters

No information regarding IESO monitoring, investigation, adjudication, or litigation is to be provided to IESO business units unless deemed warranted by a supervisor and/or legal counsel in accordance with the established process. No written or verbal communication with IESO business units is permitted unless requested or collected during the course of a matter in accordance with the established process and with approval from a supervisor or legal counsel.

Any compromises to the IESO information Confidentially Policy or these MACD practices must immediately be reported to your Supervisor.

Any information made public by MACD can be shared within the IESO.

Separation of Information from IESO

MACD is required to store all electronic information on the MACD designated servers and, where possible, convert hardcopies to electronic form for storage. These servers have access restrictions and should only allow access by MACD staff. If you notice a breach of this restriction you are to report it to your Supervisor.

Do not store MACD information on your laptop or desktop hard drive or other IESO servers that do not have restricted access.

MACD information in hard copy is to be stored in locked filing cabinets in the MACD or internal audit areas.

MACD Meetings

MACD regularly schedules teleconferences with market participants to discuss case matters. These meetings are to be held in conference rooms.

Meetings are not to take place in offices where IESO staff can overhear discussions. Where possible, in discussing case matters either book conference rooms or the MACD war room through the MACD calendar.

Transmission of Confidential Information

When available and to the greatest extent possible, the IESO portal is to be used to exchange information between external parties or contractors. This is a secure means of transmission of confidential information.

Other than documents uploaded to the IESO portal, all documents must be sent by email in PDF format password-protected. (Password-protected Word documents are also acceptable if requested by the market participant). The password is sent via a separate secure communication path other than the email with the password protected document (fax or phone). The password can also be provided over the telephone only when the contact person has been verified (eg. through voice mail message).

External parties may request information be sent without a password protection. A waiver (email confirmation) is required by the party whose information you are sending without password protection. This typically occurs as a result of technical issues (eg. firewall restrictions). Documents can also be provided on a CD with password protection through registered mail or registered courier.

Clean Desk Policy

MACD staff must ensure that MACD information is not visible in work stations when your desk is left unattended for extended period of time. Computer access should be locked if you will not be at your desk for extended periods.