**Clear Desk and Clear Screen Policy**

**1. Policy Statement**

The Clear Desk and Clear Screen Policy shall communicate the Management’s intent to protect information stored in physical and electronic media and minimize the risk of unauthorized access. Information is an asset that, like other important business assets, has value to ROYALTY EXCHANGE and consequently needs to be suitably protected. Information, in whatever form it takes, or means by which it is shared or stored, should always be appropriately protected.

**2. Purpose**

To improve the security and confidentiality of information, wherever possible a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted. This shall reduce the risk of unauthorized access, loss of, and damage to information during and outside normal working hours or when areas are unattended. The purpose of this policy is to set forth the requirements to ensure that all work areas are clear of company information, whether in electronic or paper form, classified as Level 1 – Confidential (Confidential) or Level 2 – Internal Use (Internal Use) when the work area is unattended.

**3. Definitions**

**Level 1 – Confidential Information**

Confidential information is information whose unauthorized use, access, disclosure acquisition, modification, loss, or deletion could result in severe damage to ROYALTY EXCHANGE’s employees or customers. Financial loss, damage to ROYALTY EXCHANGE’s reputation, and legal action could occur. Confidential information is intended solely for use within ROYALTY EXCHANGE’s and limited to those with a “business need-to-know”. Statutes, regulations, or other legal obligations or mandates protect much of this information. Disclosure of Confidential information to persons outside of the organization is governed by specific standards and controls designed to protect the information.

**Level 2- Internal Use Information**

Information that must be protected due to proprietary, ethical, or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of the information at this level could cause financial loss, damage to ROYALTY EXCHANGE’s reputation, violate an individual’s privacy rights or legal action could occur.

**4 Scope**

**4.1 IT Assets**

This policy applies to all  Employees, Contractors, and Third Party Employees, who have access to IT assets of ROYALTY EXCHANGE and may be bound by contractual agreements.

**4.2 Documentation**

The Policy documentation shall consist of Clear Desk and Clear Screen Policy and related guidelines.

**4.3 Document Control**

The Clear Desk and Clear Screen Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purposes.

**4.4 Records**

Records being generated as part of the Clear Desk and Clear Screen Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

**4.5 Distribution and Maintenance**

The Clear Desk and Clear Screen Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the Clear Desk and Clear Screen Policy document shall be with the CISO and system administrators.

**5 Privacy**

The Clear Desk and Clear Screen Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

**6 Responsibility**

The CISO / designated personnel is responsible for proper implementation of the Policy.

**7 Policy**

1. Computers/computer terminals shall not be left logged-on when unattended and shall be password-protected.
2. The Windows Security Lock shall be set to activate when there is no activity for three minutes.
3. The Windows Security Lock shall be password protected for reactivation.
4. Users shall shut down their machines when they leave for the day.
5. There shall be no screen savers set on for the individual’s desktops and laptops.
6. Where practically possible, paper and computer media shall be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.
7. Sensitive or classified information, when printed, shall be cleared from printers immediately.
8. The reception desk can be particularly vulnerable to visitors. This area shall be kept as clear as possible at all times.
9. Individual Personal belongings like bags, books, edibles, etc. shall be kept in drawers.
10. Before leaving for the day an individual shall make sure not to leave any paper or belongings on the desk.
11. Desktops shall have only shortcuts instead of having complete files or folders.
12. Computer screens shall be angled away from the view of unauthorized persons.
13. Physical access to the information system device that displays information shall be controlled to prevent unauthorized individuals from observing the display output.
14. Server rooms and office areas shall remain locked when they are not in use.
15. All Confidential and Internal Use information must be removed from the desk and locked in a drawer or file cabinet when the workstation is unattended and at the end of the workday.
16. All Confidential and Internal Use information must be stored in lockable drawers or cabinets.
17. File cabinets containing Confidential or Internal Use information must be locked when not in use or when not attended.
18. Keys used to access Confidential or Internal Use information must not be left in an unattended work area.
19. Laptops must be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday.
20. Passwords must not be posted on or under a computer or in any other accessible location.
21. Copies of documents containing Confidential or Internal Use information must be immediately removed from printers.

**8 Enforcement**

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy / Staff Regulation Act of ROYALTY EXCHANGE.