Real Time Risk
Safety Consulting & Services
Australia

Electronic Systems Policy Statement

Real Time Risk Safety Consulting & Services Australia (RTR SCSA) recognises the importance of providing guidance for all employees regarding the acceptable use of electronic systems, devices and the internet, and what is considered appropriate in relation to the employment relationship and in the best interests for RTR.

When using electronic systems or devices provided by RTR, employees need to ensure that any activity which is not work related, including online activity, whether done on or off RTR premises, during or outside of business hours, must not be excessive or interfere with work commitments, productivity and responsibilities.

- Reasonable use includes using internet or electronic devices for personal use as long as it does not detract from work responsibilities or accessing the internet for personal use and social media only during break times, unless otherwise permitted by your Supervisor at intermittent times.
- RTR reserves the right to monitor the 'reasonable' personal and professional use of company supplied electronic devices such as mobile phones, computers, or laptops; and access to the internet and social media; and the content of RTR email.
- It is strictly prohibited to use an unauthorised electronic device in designated areas such as facility exclusion zones or areas of high risk activity.
- Information Technology systems and networks are an integral part of Company operations. Each employee is individually responsible for the security and protection of this investment as well as the information of the Company and our Clients.
- It is not acceptable to spend hours using the internet or electronic devices that is not related to your work. If any use is seen to have an adverse impact on the performance of work, personnel will be subject to disciplinary action.
- If employees are uncertain about the appropriateness of their electronic system or device use, or the content in which they are posting online they should discuss this with their Supervisor or seek clarification from the company Code of Conduct.
- RTR reserves the right to initiate disciplinary action as necessary for any violation of this policy

Responsibilities

Each management representative, and or consultant is accountable for implementing this policy in his or her area of responsibility. This will be measured via their annual performance reviews. Management is responsible for;

- This policy is communicated and continually monitored to ensure compliance.
- Internal training is provided to all staff, employees and contractors.
- All employee's , staff and contractors are aware of the consequences that may occur if there are any breaches in relation to this policy
- The provision of resources required to meet the requirements for internet security.

Employees are to;

- Follow all company and client internet and security policies and procedures
- Report all incidents, potential security risks related to company software systems and or internet traffic to their immediate supervisor or manager.

Greg Rae
Regional Managing Director
(RTR) Safety Consulting & Services Australia
Date 04-01-2016

04 January 2016