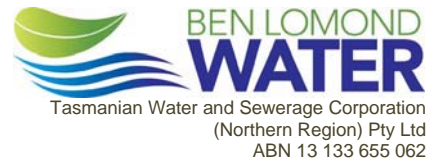


# INFORMATION SECURITY & ACCEPTABLE USE POLICY



## AIM

The Corporation will safeguard its corporate information and associated information systems to ensure business continuity, integrity and privacy of information and at the same time protect the rights of the people working for the Corporation. This policy covers the use of, access to, monitoring the usage of, disclosure, and security of corporate information that may exist in an electronic format.

## LEGISLATION

*Police Offences Act 1935*

*Copyright Act 1968*

*Privacy Act 1988*

*Freedom of Information Act 1991*

*Information Privacy Act 2000*

## POLICY

The Corporation is committed to:

- providing appropriate guidelines and induction to all employees on the security and access of information systems;
- providing appropriate measures to ensure a safe and secure work environment;
- reserving the right to monitor and inspect the usage (both business and personal) of its information systems including web browsing, e-mail and other electronic technologies;
- reserving the right to attach an appropriate disclaimer to all outgoing electronic communications;
- reserving the right to examine outgoing e-mails for inappropriate content;
- reserving the right to restrict an employee's Internet or network bandwidth if their usage is having a detrimental impact on overall system performance or is deemed by their supervisor to be excessive;
- reporting any illegal activities to the appropriate authorities; and
- responding to any breaches of this policy in an appropriate manner.

Employees, subcontractors, and consultants will:

- not use the information systems inappropriately (as defined in any Information Security and Acceptable Use Guidelines);
- employ safe and secure work practices when using the information systems;
- be aware that all information system usage (both business and personal) may be monitored and investigated for inappropriate activity;
- observe the allocated allowance of personal internet time/downloads per month;
- be responsible for filing into the Electronic Document & Records Management System (EDRMS) all business documents and e-mails in accordance with relevant guidelines;

- inform the recognised Discrimination and Harassment Contact Officer if any unwanted, inappropriate or offensive electronic communication is received;
- not modify or remove the disclaimer attached to any outgoing electronic communications being sent to an external party in any way;
- respond to any relevant electronic communications received from an external party within ten business days;
- respect the rights of other employees, subcontractors, and consultants in respect to the privacy of information; and
- only use electronic communications (as defined) for personal purposes in their own time and, to the extent approved by the Chief Executive Officer, ensure that the usage conforms to this policy and applicable guidelines, and does not interfere with the performance of their or any other person's duties.

## RESPONSIBILITIES

The CEO is responsible for ensuring that the Corporation complies with applicable legislation.

All staff are required to comply with the spirit and letter of this policy and its associated procedures and undertake any relevant training as required.

## REFERENCES

Information Security and Acceptable Use Guidelines

Corporate Code of Conduct

*Approved by the Board on 10 August 2010*

Signed:

  
\_\_\_\_\_  
Chief Executive Officer