

**State Water Policy: 09/354****Contractor Access Policy**

This policy aims to ensure that:

- All personnel that engage contractors are aware of their responsibilities for the duration of the contract.
- Contractors engaged are aware of their site, systems and data access abilities and requirements.

**Scope**

This policy outlines the responsibilities and expectations of any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. Also outlined is the responsibilities and expectations of the State Water personnel responsible for the contracting and/or supervising of the third party. A third party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and security companies.

**Computer Room Third Party Policy Guidelines**

1. All third-party access to the computer room should be scheduled to occur during regular business hours. If this is not possible, a point person from the IT department will be scheduled after hours to accompany the third party.
2. When third parties are scheduled to have access to the computer room, the Information Services staff must be notified in advance of the date, time, and type of work to be performed.
3. When the third party arrives, he/she will report to a staff contact that scheduled the visit. The staff contact will escort the third party to the Information Services area. At this point, the third party is to be informed that he/she will take further direction from the IT staff point person in relation to their activity in the computer room.
4. Prior to the onset of any work, the third party will describe the activities that are planned
5. The IT staff point person is responsible for explaining what measures need to be taken to protect the computer hardware and software, explain protective measures to the third party, and ensure that the measures come to fruition. In an attempt to offset delays in the work of the third-party individual(s), the IT staff will attempt to minimize the delays within the constraint of safeguarding the systems. The third party will need to clearly understand that they are to allow time for the IT staff to do what needs to be done to protect the computer systems before starting their work.
6. The third party will report to and receive instructions from the IT staff point person regarding their work in the computer room. The IT staff point person will also be kept informed of the status of the work, as well as the notification that the work is completed before leaving the area.

## ***Contractor Access Policy***

---

### **Information Systems Third-Party Policy Guidelines**

1. Any third-party agreements and contracts must specify:
  - The work that is to be accomplished and work hours. Also, any configuration information of any installed software as well as virus checking of that software.
  - The State Water data and information that the third party should have access to.
  - The minimum security requirements that the third party must meet (i.e., method for remote access).
  - How State Water data/information is to be guarded by the third party. Signing of a confidentiality agreement is typically required.
  - Strict use of State Water data/information and information resources for the purpose of the business agreement by the third party. Any other State Water information acquired by the third party in the course of the contract cannot be used for the third-party's own purposes or divulged to others.
  - Feasible methods for the destruction, disposal, or return of State Water information at the end of the contract.
  - The return of company property such as a laptop, PDA, or cell phone after the completion or termination of the agreement.
2. The third party must comply with all applicable State Water standards, agreements, practices and policies, including, but not limited to:
  - Acceptable use policies.
  - Software licensing policies.
  - Safety policies.
  - Auditing policies.
  - Security policies.
  - Non-disclosure policies.
  - Privacy policies.
3. State Water will provide an IT point of contact for the third party whether it is one person from the IT department or an interdepartmental team. This point of contact will liaise with the third party to ensure they are in compliance with these policies.
4. The third party will provide State Water with a list of all additional third parties working on the contract. The list must be updated and provided to State Water within 8 hrs of any staff changes.
5. Third party access to systems must be uniquely identifiable and authenticated, and password management must comply with the State Water Password Control Policy. Managing connectivity with partner networks can be handled different ways depending on what technologies are in place (i.e. encryption, intrusion detection, DMZ architecture).
6. Third party computer/laptop/PDA/tablet PC will not be allowed to connect to the State Water systems. The third party will be held accountable for any damage

---

**FOR INTERNAL USE ONLY**

## Contractor Access Policy

occurred to State Water in the event that an incident occurs where use of their own equipment has occurred.

7. If applicable, each third party on-site employee must acquire an ID badge that must be displayed at all times while on the premises. The badge must be returned to State Water upon termination or completion of a contract.
8. Each third-party employee that has access to sensitive information should be cleared to handle that information.
9. If applicable, an explanation of how information will be handled and protected at the third party's facility/site must be addressed.
10. Third-party employees must report all security incidences to the appropriate State Water personnel.
11. If third-party management is involved in a State Water security incident management, the responsibilities and details must be specified in the contract.
12. The third party must follow all applicable change control procedures and processes.
13. All software used by the third party in providing service to State Water must be properly inventoried and licensed.
14. All third-party employees are required to comply with all applicable auditing regulations and State Water auditing requirements, including the auditing of the third-party's work.
15. Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by the appropriate State Water management.
16. All third-party maintenance equipment on the network that connects to the outside world via telephone lines, leased line, or the network will remain disabled except when in use for authorized maintenance.
17. The third party's major accomplishments must be documented and available to State Water management upon request. Documentation should include, but is not limited to events such as:
  - Personnel changes.
  - Password changes.
  - Project milestones.
  - Deliverables.
  - Arrival and departure times.
18. Upon departure of the third party from the contract for any reason, the third party will ensure that all sensitive information is collected and returned to the company or destroyed within 2 hrs. The third party will also provide written certification of that destruction within 4 hrs. All equipment and supplies must also be returned, as well as any access cards and identification badges. All equipment and supplies retained by the third party must be documented by authorized State Water management.

---

**FOR INTERNAL USE ONLY**

## ***Contractor Access Policy***

---

19. State Water will perform an impact analysis of other business-critical functions, once work has begun by the third party.
20. State Water will monitor system and network log files 3 times per week.
21. State Water will eliminate third-party physical access to facilities after the contract has been completed or terminated. The following steps must be performed:
  - Remove third party authentication and all means of access to systems.
  - If needed, make sure that incoming e-mail is re-routed to an appropriate person.
  - Archive any third-party software configuration, and transfer ownership to designated internal staff.
  - Get a written statement from the third party that any software created and/or installed by the third-party is free of viruses and any other malicious code.

### **Procedures**

Contractor access will only be granted once all authorised contracts and confidentiality agreements have been sighted by the Chief Information Officer. The Chief Information Officer will then authorise the IT Administrator to grant the contractor the required access.

### **Policy Administration**

The responsibility and authority to implement and enforce this policy rests with each Manager who has contractors. This responsibility includes effective communication of the policy and any necessary related procedures to all affected staff. Approval to deviate from this policy can be given only by the Chief Information or Chief Executive Officer.

### **Feedback**

Feedback on this policy is welcome. Feedback and enquiries in relation to this policy should be directed to the Information Services Branch on (02) 6841 2084.

**Adopted by:** Management Team, 05 May 2009

**Issued by:**  
Sandra Coleman  
Chief Information Officer  
(02) 6841 2071

**Issue Date:** 05 May 2009  
**Issued to:** All State Water staff

**Review date:** 05 May 2010 [12 months after adoption]

---

#### **FOR INTERNAL USE ONLY**