



IT Security

Security and Standards

ac3's data centres and services are maintained in a secure manner. The **ac3** security procedures and policies are developed on a baseline that uses ACSI 33 and an ISO 27001 certified process. The previous AUS/NZ 7799:2003 certification was migrated to ISO27001 with integration into the **ac3** Solution Delivery Process to ensure that every customer's security needs are clarified prior to service delivery.

This systematic approach involves attention to identified business needs and aspects of physical, logical and management security and responsibility. Physical provisions include personnel access controls — such as the “escorted visitor” policy, special physical construction and layouts, video surveillance, 7x24x365 security patrols and environmental monitoring. Logical security can include layered firewalls, enforced policy change management, e-mail screening, specialised virus protection, secure LAN segmentation, layered access controls to systems, secure storage and token-based authentication for user access.

All networked devices are constantly monitored and **ac3** uses a purpose built network surveillance system to detect incidents and failures and alert operational staff on a 24x7 basis.

Logical Security

Perimeter Security

ac3 has state of the art firewall systems to protect both at a packet and application level against unauthorised access from the Internet. Customer input is essential to choosing an appropriate security level to meet business needs with security certified staff available to assist in deciding the best solution. Specialised security zones are established throughout the **ac3** network environment to enable selective reduction in risks both from the Internet and local systems. These zones are all firewalled with logging of connectivity between them.

Secure Access

Users are encouraged to use secure protocols for communication within their environments located at **ac3**. **ac3** staff can advise customers on the latest and most secure forms of communication to ensure privacy and security are maintained when connecting to their systems.

Security Audit and Security “hardening”

ac3 enforces a security audit and security “hardening” process on systems placed in the **ac3** data centres that use shared services, such as Internet access or backup. This is performed to ensure that a minimal but risk adverse level of security is maintained for all customers.

Backup

A shared backup service is available for customers. Backups are carried out incrementally on a daily basis, with a full backup weekly. Backup tapes are stored off-site on a weekly basis.

ac3 can provide, maintain or design a secure backup system that allows customer data to be treated with the appropriate level of Confidentiality and Integrity in addition to providing an increased level of Availability in the event of system disruption.

Responsibility and Incident Reporting

The Security Manager is responsible for the security of the data centres. This responsibility cannot be delegated. The Security Manager, on approval from the CEO, reserves the right to suspend any customer service on detection of a security breach.

All security breaches and alerts should be reported to the Security Manager as soon as practicable, but remedial and emergency actions may be taken by others in accordance with policy and operating procedures. Reporting of security breaches to the proper legal entities is encouraged by **ac3**, however such incidents are treated with respect to the customers appropriate security policy and business requirements.

Physical Security

Surveillance

The **ac3** perimeter at the ATP data centre is monitored by 24x7x365 security patrols by security personnel certified to Australian standards. The guards are empowered to challenge all unauthorised people found in or near the **ac3** facility and all have a minimal certification of 1A and 1C. Video surveillance in the data centre allows the security service to monitor the data centre at all times.

The Global Switch data centre has comprehensive 24x7x365 security on site, with man traps for access past the lobby area.

Environmental Monitoring

All environmental variables — air temperature, humidity, power into and out of the UPS, fire detection systems, under-floor water detection — are monitored continuously. Additionally **ac3** has invested in a comprehensive “to rack” power monitoring capability to ensure power availability is maintained and recorded.

In the event of an alert **ac3** staff on site are warned by audio/visual alarm panel. Status reports and alarm conditions are duplicated and sent to the on-site 24 x 7 security service to ensure that alerts are dealt with as a priority. Outside business hours a pager system informs the duty operations specialist and this has automatic escalation as a precautionary measure.

Access to Data Centres

There is no general access to the data centres. On special occasions visitors may be escorted through the data centres at the discretion of the CEO.

ac3 has an “escorted visitor” policy, where visitors are accompanied by **ac3** staff at all times. The **ac3** escort is a technically competent person capable of judging the activities for their potential damage, and is not a security guard or clerical staff.

ATP Data Centre: Personnel entry is by means of three locked doors, including a double key padded airlock. The equipment entry is a double door protected by security mesh and bollards. To access the computer room one must have a Smartcard for the front door, as well as the combinations for the electronic lock and the mechanical combination lock in the airlock.

Global Switch Data Centre: Regular visitors, such as **ac3** staff, are provided with access cards. Before gaining access to the Global Switch lobby, visitors identify themselves through a security camera and intercom, and finally gain access to the lobby at the instigation of Global Switch Security. Visitors need a valid escort to proceed further, and are checked against an approved list for whom 24 hours notice has been provided. Visitors finally gain access to the main data centre, accompanied by their nominated escort, through a man trap. Access to particular areas in the Global Switch complex is via swipe cards.

ooOoo