



# IT Security

## ***Security and Standards***

The **ac3** data centres are highly secure, and as a result **ac3**'s customers and stakeholders can be assured that all infrastructure entrusted to **ac3** is managed in accordance with current best practice. The **ac3** security policy is based around ACSI 33, AS 4360, AS/NZS 7799.2:2003 and AS/NZS 4444 standards.

The standards-based approach involves attention to all relevant aspects of physical and logical security. Physical provisions include access controls — such as the “escorted visitor” policy, the physical construction and layout of the data centres, video surveillance, 7x24x365 security patrols and environmental monitoring. Logical aspects of security include layered firewalls, enforced policy, e-mail screens and virus protection, LAN segmentation, access controls to computers and storage, and token-based strong authentication for user access when required.

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

## ***7799 Security Accreditation***

The ATP data centre is currently certified to the AS/NZS 7799.2:2003 standard, and is in the process of upgrading to ISO 27001:2005. The improved process management for the **ac3** security regime, through evolving to this standard, enables **ac3** to provide our customers with an appropriate risk-based approach to security.

## ***Logical Security***

### ***Perimeter Security***

**ac3** has a secure gateway mechanism available with multiple firewalls to protect both the packet and application levels against unauthorised access from the network. Customers can choose an appropriate security level to meet their business needs. The local area network is divided into trusted and untrusted domains, protected from one another by firewall services.

### ***Highly Secure Access***

For highly secure access, token based authentication is available. Registered users are provided with a PIN protected authentication token which generates time-locked one-time-passwords (i.e. passwords that can be used only once and are valid only for a short period).

**ac3** users are encouraged to use secure protocols for communication with their services located within the **ac3** data centres. **ac3** staff can assist customers on the best practice means and software available to ensure secure communication.

### ***Security Audit and Security “hardening”***

**ac3** enforces a security audit and security “hardening” on any server placed in **ac3**'s data centres that uses shared services, such as Internet access or the shared backup facility. This is done to ensure that an adequate level of security is in place 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 carry out backups for customers using their own backup systems or establish an independent backup system if requested.

### **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 guarded by 24x7x365 security patrols, who make frequent, but randomly spaced, patrols. The guards are empowered to challenge all unauthorised people found in or near the **ac3** facility. Video surveillance in the data centre allows the security service to monitor the data centre at all times.

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

#### **Environmental Monitoring**

All systems — air temperature and humidity, power in and out of the UPS, status of fire detection systems, under-floor water detection and other environmental systems are monitored continuously. In the event of an alert **ac3** on-site personnel are warned by audio and visual alarm panel. Status reports and alarm conditions are also monitored by the on-site security service which is monitored 24 x 7 x 365. Outside core 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 usual rules apply to activities permitted in the machine room including NO food, drink, smoking, use of chemical solvents or other activities considered to possibly cause damage to either personnel or the computing resources. The escort present with any visitor 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:** Entrance is by means of three locked doors — a fire exit accessible from the inside only, a double door for equipment delivery protected by a purpose built security mesh padlocked to the floor, and the operational entry via the Operations area air-lock. To access the computer room one must have a Smartcard for the front door, the combination for the electronic lock on the air-lock and the combination to the mechanical combination lock on the computer room door.

**Global Switch Data Centre:** At least 24 hours notice must be provided for visitors to access the Global Switch building. 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