Cyber Security & Compliance Checklist

Software	**RollCall Safety Solutions**
Department/User	
Source reference	**RollCall Whitepaper – Security & Compliance**
Completed by & date	**Craig McIntyre 17.09.2025**

***Mandatory Requirement**

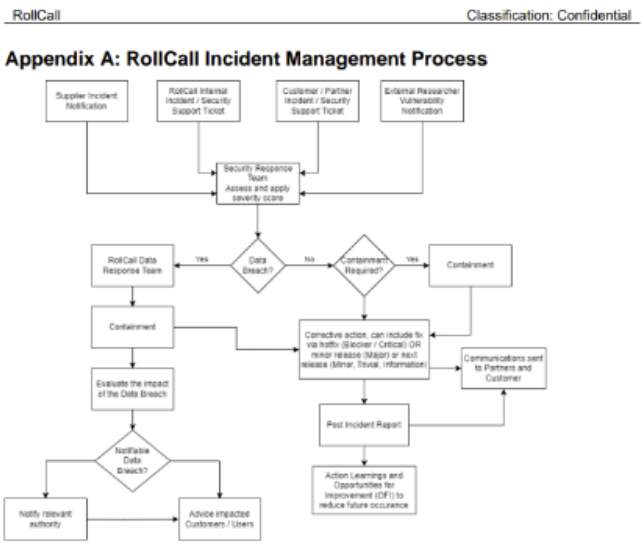
Item	Conforms (Y/N)	Notes. Provide bullet points of your implementation. If (N) describe mitigation measures
Organisational Security - Explain the measures in place.		
Employee background Check	Y	Each employee undergoes a process of background verification – including Working with Children Check.
Security Awareness	Y	Each employee, when inducted, signs a confidentiality agreement and acceptable use policy, after which they undergo training in information security, privacy, and compliance.
Dedicated security and privacy teams	Y	Have dedicated security and privacy officers that implement and manage the programs.
Internal audit and compliance	Y	Internal and External audits to ensure ISO 27001 compliance
Endpoint Security*	Y	All staff workstations are tracked, monitored and patches are enforced by on device policy.
Physical Security - Do you have approved policies on the following		
At the workplace	Y	Yes, as per ISO27001 Asset Management Policy, this includes the following criteria: 7.0 **Physical and Environment Security** 7.1 **Secure Areas** 7.1.1 Physical Security Perimetre 7.1.2 Physical Entry Controls 7.1.3 Securing Offices, Rooms and Facilities 7.1.4 –Protecting Against External and Environmental Threats 7.1.5 Working in Secure Areas 7.2 **Equipment**

Item	Conforms (Y/N)	Notes. Provide bullet points of your implementation. If (N) describe mitigation measures
		7.2.1 – Equipment Siting & Protection 7.2.2 – Supporting Utilities 7.2.3 – Cabling Security 7.2.4 – Equipment Maintenance 7.2.5 – Removal of Assets 7.2.6 – Security of Equipment and Assets off Premises 7.2.7 – Secure Disposal or Re-use 7.2.8 – Unattended User Equipment 7.2.9 – Clear Desk & Clear Screen Policy.
At the data Centres*	Y	AWS Sydney data centres feature 24/7 security personnel, biometric access controls, multi-factor authentication, video surveillance, mantrap entry systems, and restricted access zones. Facilities are unmarked with perimeter security and environmental controls.
Monitoring*	Y	Continuous 24/7 monitoring with security operations centres, real-time video surveillance, motion detection systems, environmental monitoring (temperature, humidity, power), and automated alerting. All access events are logged and audited with AWS maintaining SOC 1, SOC 2, and ISO 27001 compliance.
Infrastructure security		
Network Security/Redundancy*	Y	Multi-AZ deployment across Sydney availability zones with VPC isolation, security groups, NACLs, and AWS WAF. Load balancers distribute traffic with auto-scaling groups for redundancy.
Server hardening*	Y	EC2 instances follow CIS benchmarks with minimal software installation, regular patching via Systems Manager, disabled unnecessary services, and IAM roles with least privilege access.
Intrusion detection and prevention*	Y	AWS GuardDuty for threat detection, CloudTrail for API auditing, Intruder.io for autopen, AWS Inspector for vulnerability checks, SSL labs for Data encryption checking
Data Security - Explain your practice on the following		
Data Residency (Held in AUS/NZ) *	Y	All data stored exclusively in AWS Asia Pacific (Sydney) region (ap-southeast-2) ensuring Australian data residency compliance.
Data Encryption – at rest*	Y	All storage encrypted using AWS KMS with customer-managed keys - S3 buckets, RDS databases, and MongoDB.
Data Encryption – In transit*	Y	LS 1.2+ for all communications, HTTPS endpoints, encrypted database connections, and VPN/Direct Connect for internal traffic.

Item	Conforms (Y/N)	Notes. Provide bullet points of your implementation. If (N) describe mitigation measures
Data Backup/Recovery*	Y	Automated constant snapshots using AWS Backup, cross-AZ replication, point-in-time recovery for databases, and tested disaster recovery procedures with defined RTO/RPO.
Data Retention/Disposal	Y	1. **Client Off-Boarding Workflow** *Day 0 – Termination Confirmed* ○ Send final invoice & Termination Pack. ○ Enable read-only mode. *Day 0 → 30 – Grace Period* ○ Client self-service export (CSV/JSON + PDF reports). *Day 30 – Access Removal* ○ Disable all logins; rotate shared API keys. *Day 30 → 60 – Archive Period* ○ Snapshot tenant DB; move encrypted snapshot to S3 Glacier/"off-board" bucket. 2. **Data Destruction** ○ Annual purge job executed via scheduled Lambda in the first week of February. The job deletes only rows who's 'deleted at' timestamp is **≥ 365 days** old, guaranteeing the ENSY+1Y buffer. ○ Job performs: ▪ **Soft-delete** flagging (24 h rollback window). ▪ **Hard-delete** cascade (SQL) + TTL trigger (Mongo). ▪ Redaction of message bodies in ticketing DB. ▪ Post-run audit: record row-count delta and SHA-256 checksum in data_purge_audit table. 3. **Evidence & Audit** ○ Purge job logs stored in immutable S3 bucket (audit-bucket) with Object Lock. ○ Quarterly internal audit to sample and verify compliance.
Identity and Access control - does your system allow		
Single Sign-On*	Y	SAML 2.0 SSO integration supported with enterprise identity providers including Active Directory Federation Services (ADFS), Azure AD, Okta, and Google Workspace.

Item	Conforms (Y/N)	Notes. Provide bullet points of your implementation. If (N) describe mitigation measures
MFA*	Y	Configurable Multi-Factor Authentication for all administrative accounts with support for SMS and email verification.
What level of Admin Access*	Y	Role-based access control (RBAC) with granular permission levels including School admin, Third party, Read Only. All access follows principle of least privilege with audit logging.
Operational Security - Explain the measures in place		
Logging and Monitoring	Y	Centralised logging via AWS CloudTrail, CloudWatch, and VPC Flow Logs with real-time monitoring dashboards. Automated alerting for suspicious activities, failed login attempts, and policy violations with 24/7 monitoring coverage.
Vulnerability management	Y	Regular vulnerability scanning using AWS Inspector and third-party tools including intruder.io.
Malware and spam protection	Y	Multi-layered protection including AWS WAF, endpoint detection and response (EDR) on all systems.
DR and BCP*	Y	Yes, as per ISO27001 Business Continuity Management Policy, this includes the following criteria: **6.0 Business Continuity Planning Process** 6.1 Business Impact Analysis (BIA) Summary 6.2 BIA Approach 6.3 Dependencies 6.4 Business Continuity Planning 6.5 Information Security During Disruption 6.6 ICT Readiness for Business Continuity 6.7 Redundancy of Information Processing Facilities 6.8 Disaster Prevention 6.9 Business Continuity Testing 6.10 Review
Incident management		
Explain your incident reporting process	Y	We use the ISO27001 incident management policy. See below contents of the policy: 5.0 Responsibilities and Authorities 5.1 Security Response Team 5.2 Data Response Team 6.0 Information Security Incidents and Breaches 7.0 Assessment and Decisions **8.0 Response to Information Security Incidents** 8.1 Information Security Corrective Action 8.2 Data Response Containment 8.2.1 Data Response Impact Analysis 8.2.1.1 The Type of Information Involved

Item	Conforms (Y/N)	Notes. Provide bullet points of your implementation. If (N) describe mitigation measures
		8.2.1.2 Determine the context of the affected information and breach 8.2.1.3 Establish the cause and extent of the breach 8.2.2 Assess the risk of harm to the affected persons 8.3 Data Breach Notification 8.3.1 Notification Process to Authorities 8.3.2 Other Notifications 9.0 Collection of Evidence 10.0 Learning from Information Security Incidents.
Do you have a process for Vendor and Third-Party Supplier Management?	Y	Yes, as per ISO27001 Supplier Management Policy, this includes the following criteria: 6.0 **Supplier Management** 6.1 Internal Communication 6.2 Critical Supplier List 6.3 Confidentiality and Non-Disclosure Agreement 6.4 Supplier Assessment Record 6.5 Information Security in Supplier Relationship 6.5.1 Information Security Policy and Supplier Relationship 6.5.2 Addressing Security within Supplier Relationship 6.5.3 Information and Communication Technology Supply Chain 6.6 Supplier Service Delivery Management 6.6.1 Monitoring and review of Supplier Services 6.6.2 Managing Changes to Supplier Services 6.7 Supplier Disqualification

Item	Conforms (Y/N)	Notes. Provide bullet points of your implementation. If (N) describe mitigation measures
How do you manage a breach notification process*		
Operational Security	Y	Logging and Monitoring,