Stratos Cyber

Third-Party Cybersecurity Contract Checklist

Caribbean Organizations • Boards & Executive

Use this checklist during vendor selection, contract negotiation, and ongoing governance. These items are non-negotiable for any third party

1 VENDOR SELECTION – NON-NEGOTIABLES

- *Alignment to a recognized framework (ISO 27001, NIST, CIS or equivalent)*
- *Strong identity & access controls, incl.*
  - *MFA for privileged/remote access*
- *Defined breach & incident notification timeline (contractual, not best-effort)*
- *Clear data ownership, approved data locations & cross-border data disclosure*
- *Explicit right to audit cybersecurity controls (vendor refusal is disqualifying)*
- *Commitment to cooperate during incidents, investigations & regulatory response*

2 MANDATORY CONTRACT CLAUSES

- *Documented cybersecurity obligations and minimum control requirements*
- *Formal incident escalation procedures with named contacts & response timelines*
- *Right to scheduled and event-triggered audits, incl. independent assurance reviews*
- *Contractual responsibility for subcontractors and fourth parties*
- *Clear accountability for negligent security practices (liability may be capped; responsibility must not be)*
- *Exit and termination clauses covering secure data return or certified destruction*

3 LIFE-OF-CONTRACT GOVERNANCE REQUIREMENTS

- *Periodic cybersecurity posture and third-party risk reviews*
- *Mandatory notification of material changes (scope, data location, subcontractors)*
- *Participation in incident response testing or tabletop exercises when requested*
- *Tracked remediation of audit findings with defined timelines*
- *Post-termination cooperation for incidents related to the contract period*

4 C and BOARD-LEVEL ACCOUNTABILITY CHECK

- *Cyber risk ownership remains with management and the board — not the vendor*
- *Third-party cyber risk is reviewed as part of enterprise risk management*
- *Vendor reporting is understandable at executive and board level*
- *Cybersecurity effectiveness is measured by business impact, not tools deployed*

■ **GOVERNANCE REMINDER**:
Cyber risk ownership remains with your organisation not the vendor. This checklist does not transfer accountability.

Stratos-cyber.com
info@stratos-cyber.com