<table>
<thead>
<tr>
<th>Commandment #1</th>
<th>Commandment #2</th>
<th>Commandment #3</th>
<th>Commandment #4</th>
<th>Commandment #5</th>
<th>Commandment #6</th>
<th>Commandment #7</th>
<th>Commandment #8</th>
<th>Commandment #9</th>
<th>Commandment #10</th>
<th>Commandment #11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 17 (1), (2), (3), (4)</td>
<td>NIST SP 800-53 R3</td>
<td>CP-1</td>
<td>CP-2</td>
<td>CP-3</td>
<td>CP-4</td>
<td>CP-5</td>
<td>CP-6</td>
<td>CP-7</td>
<td>CP-8</td>
<td>CP-9</td>
</tr>
<tr>
<td>6.04.03. (a)</td>
<td>NIST SP 800-53 R3</td>
<td>PE-1</td>
<td>PE-4</td>
<td>PE-13</td>
<td>PE-13 (1)</td>
<td>PE-13 (2)</td>
<td>PE-13 (3)</td>
<td>PE-13 (4)</td>
<td>PE-13 (5)</td>
<td>PE-13 (6)</td>
</tr>
<tr>
<td>6.07. (b)</td>
<td>ISO/IEC 27001</td>
<td>56 (B)</td>
<td>56 (C)</td>
<td>56 (D)</td>
<td>56 (E)</td>
<td>56 (F)</td>
<td>56 (G)</td>
<td>56 (H)</td>
<td>56 (I)</td>
<td>56 (J)</td>
</tr>
<tr>
<td>6.07. (c)</td>
<td>ISO/IEC 27002</td>
<td>56 (B)</td>
<td>56 (C)</td>
<td>56 (D)</td>
<td>56 (E)</td>
<td>56 (F)</td>
<td>56 (G)</td>
<td>56 (H)</td>
<td>56 (I)</td>
<td>56 (J)</td>
</tr>
<tr>
<td>6.07. (d)</td>
<td>ISO/IEC 27001</td>
<td>56 (B)</td>
<td>56 (C)</td>
<td>56 (D)</td>
<td>56 (E)</td>
<td>56 (F)</td>
<td>56 (G)</td>
<td>56 (H)</td>
<td>56 (I)</td>
<td>56 (J)</td>
</tr>
<tr>
<td>6.07. (e)</td>
<td>ISO/IEC 27002</td>
<td>56 (B)</td>
<td>56 (C)</td>
<td>56 (D)</td>
<td>56 (E)</td>
<td>56 (F)</td>
<td>56 (G)</td>
<td>56 (H)</td>
<td>56 (I)</td>
<td>56 (J)</td>
</tr>
<tr>
<td>Clause 4.3.3</td>
<td>A.10.5.1</td>
<td>A.10.7.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>------------</td>
<td>------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Do you have a capability to use system geographic location as an authentication factor?
- Do you test your backup or redundancy mechanisms at least annually?
- Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?
- Do you have controls in place to ensure that standards of quality are being met for all software development?
- Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?
- Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?
- Do you have technical control capabilities to enforce tenant data retention policies?
- Do you provide customers with ongoing visibility and reporting of your SLA performance?
- Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?

<table>
<thead>
<tr>
<th>Commandment #1</th>
<th>Commandment #2</th>
<th>Commandment #3</th>
</tr>
</thead>
</table>

- There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud or on-premises) on mission-critical business operations. This method includes consideration of the impact on the achievement of recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption.
- Responsibility and accountability for the entity’s system availability, confidentiality of data, processing integrity, system security and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them. Relevant personnel is to be educated and trained on all applicable policies, procedures and updates. Applicable personnel are responsible for adhering to these policies and procedures.
- Policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring the integrity of backup data and systems maintained to ensure the availability of backup data and systems in the event of recovery measures being incorporated as part of business continuity planning and tested accordingly for effectiveness.

<table>
<thead>
<tr>
<th>BCR-11.2</th>
<th>Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3</th>
</tr>
</thead>
</table>

- Measures to prevent or mitigate threats (A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability, confidentiality of data, processing integrity, system security and related security policies.(A3.4.0) Procedures exist to provide for the integrity of backup data and systems maintained to ensure the availability of backup data and systems in the event of recovery measures being incorporated as part of business continuity planning and tested accordingly for effectiveness.

<table>
<thead>
<tr>
<th>SRM &gt; Policies and Standards &gt; Operational Security Baselines</th>
</tr>
</thead>
</table>

- Change Control & Configuration Management (C3.14.0)

- Data Security & Information Lifecycle Management (C3.2)

- Identity and Access Management (C3.8.0)

- Service Continuity (C3.10.0)

- Service Delivery (C3.11.0)

- Service Level Management (C3.12.0)

- Service Measurement (C3.13.0)

- Service Obligation (C3.14.0)
### Are users made aware of their responsibilities for maintaining a safe and secure working environment?

- Do the above procedures and guidelines account for timely revocation of access and return of assets?

### Do you review your Information Security Management Program (ISMP) least once a year?

- Do you make available documentation of your organization-wide risk management program?

---

<table>
<thead>
<tr>
<th>Clause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5A.6.1.1</td>
<td>Responsibility and accountability for IS-02 COBIT 4.1 DS5.1 APO01.02</td>
</tr>
<tr>
<td>4.44.2(b)</td>
<td></td>
</tr>
<tr>
<td>6.1.2(a)</td>
<td></td>
</tr>
<tr>
<td>6.2(a)</td>
<td></td>
</tr>
<tr>
<td>6.2(d)</td>
<td></td>
</tr>
<tr>
<td>7.1</td>
<td></td>
</tr>
<tr>
<td>7.4</td>
<td></td>
</tr>
<tr>
<td>9.3</td>
<td></td>
</tr>
<tr>
<td>10.2</td>
<td></td>
</tr>
<tr>
<td>7.2(b)</td>
<td></td>
</tr>
<tr>
<td>7.2(c)</td>
<td></td>
</tr>
<tr>
<td>7.2(d)</td>
<td></td>
</tr>
<tr>
<td>7.3(b)</td>
<td></td>
</tr>
<tr>
<td>7.3(c)</td>
<td></td>
</tr>
</tbody>
</table>

---

| Article 17 NIST SP 800-53 R3 AC-1 | |
| R2.1 - R2.2 - | |

---

| I dipendenti hanno firmato un documento denominato “EasyAcademy – Piano di consapevolezza dei dipendenti sulla sicurezza informatica” e il “Piano di sensibilizzazione dei dipendenti sulla sicurezza informatica.” I documenti sono disponibili a richiesta dei clienti, gli SLA sono esplicitati nel contratto di fornitura. |

---

| CBGP PCI DSS v2.0 12.7 | |

---

| 45 CFR 164.316 (b)(2)(iii) | |

---

| Governance and Risk Management GRM-06.3 | |
| GRM-07.1 | |

---

| Governance and Risk Management | |

---

| BOSS > Human Resources Security > Employee Termination S1.1.0 (S1.1.0) The entity’s security policies are established and periodically reviewed and approved |

---

| IS-27 Domain 2 Article 17 NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-4 5.2.3 7.2.2 8.2.1 8.2.6 | |

---

| HRS-03.4 | |
| HRS-04.1 | |
| E.6 HR-03 COBIT 4.1 PO 7.8 None Article 17 NIST SP 800-53 R3 PS-2 | |

---

| Governance and Risk Management | |

---

| BOSS > Compliance S3.11.0 (S3.11.0) Procedures exist to help ensure that personnel responsible for the design, development, operation, maintenance, or modification of the information system are appropriately aware of, and adhere to, their responsibilities for protecting the physical security of the information system and the information it supports |

---


---

| Services > Presentation Platform > Endpoints - Mobile Devices - Mobile Device Management | |

---

| Governance and Risk Management | |

---

| Governance and Risk Management | |

---

### Are requirements for non-disclosure or confidentiality agreements reflecting the organization’s needs for the protection of data and operational details identified, documented and reviewed at planned intervals?

- Are the requirements for non-disclosure or confidentiality agreements reflecting the organization’s needs for the protection of data and operational details identified, documented and reviewed at planned intervals?

---

| Acceptable Use | |

---

| Training / Awareness | |

---

| Acceptable Use | |

---

| User Responsibility | |

---

| User Responsibility | |
The text content from the image is not clearly visible due to the nature of the table. However, it appears to be a matrix with various columns and rows, likely representing some form of data analysis or comparison. The specific content and context are not discernible from the image provided.
Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?

Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?

For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?

Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?

Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling ... traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?

Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?
Mobile Security

Approved Applications

Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?

Does your BYOD policy and training clearly state which applications and application stores are approved for use on BYOD devices?

The company shall have a documented mobile device policy that approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.

All cloud-based services used by the company's mobile devices or cloud-based services that store provider managed data must be approved through the company's BYOD policy.

Do you have a documented application validation process for testing device, operating system and application compatibility issues?

The company shall have a documented application validation process.

The BYOD policy shall define the device and eligibility requirements allowed for BYOD usage.
Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?

Does your logging and monitoring framework allow isolation of an incident to specific tenants?

Do you have a documented security incident response plan?

Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?

Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (OS system and patch levels, lost or decommissioned, device assignee)?

Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?

Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?

Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?

Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?

Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?

Contact / Authority Maintenance

Points of contact for applicable regulation authorities, national and local law enforcement, and other legal responsibilities have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.
Do you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?

Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?

Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) services shall be designed, developed, and deployed in accordance with:

- Forensics regarding breaches of the system security and for submitting:
  - NIST SP 800-53 R3 AU-7
- Security Incident Management, E-Discovery & Cloud Forensics:
  - NIST SP 800-53 R3 PS-7
  - NIST SP 800-53 R3 SA-6
  - NIST SP 800-53 R3 SA-7
  - NIST SP 800-53 R3 SA-9

- Incident Response:
  - Clause 6.1.1, 6.1.1(e)(2), 6.1.2, 6.1.2(a)(1), 6.1.2(a)(2), 6.1.2(b), 6.1.2(c), 6.1.2(c)(1), 6.1.2(c)(2), 6.1.2(d), 6.1.2(d)(1), 6.1.2(d)(2)

- Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following:
  - Article 17 NIST SP 800-53 R3 SC-5

- Effectively governance, risk management, assurance and legal,:
  - Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3

- The availability, confidentiality of data, processing integrity, system security and related security policies and procedures:
  - S2.2.0

- Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, and data transmission:
  - NIST SP 800-53 R3 AC-1
  - NIST SP 800-53 R3 AT-1
  - NIST SP 800-53 R3 AU-1
  - NIST SP 800-53 R3 CA-1
  - NIST SP 800-53 R3 CM-1

- Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain:
  - Partial, 8.1* partial, A.15.1.2, 8.1* partial, A.15.2.1, A.13.1.2, A.12.2.1

- Third-party service providers shall conduct vulnerability scanning and periodic penetration testing on your applications and networks:
  - A.10.4.1 Commandment #4
  - A.10.4.2 Commandment #5

- Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, data transmission and references to detailed supporting and relevant business processes and technical measures implemented to enable:
  - A.10.8.2
  - A.11.4.6
  - A.11.6.1
  - A.12.3.1
  - A.12.5.4

- Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, data transmission and references to detailed supporting and relevant business processes and technical measures implemented to enable:
  - A.6.2.3
  - A10.2.1
  - A.11.2.1

- Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, data transmission and references to detailed supporting and relevant business processes and technical measures implemented to enable:
  - A.14.1.6
  - A.14.6.1

- Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, data transmission and references to detailed supporting and relevant business processes and technical measures implemented to enable:
  - A.15.1.2
  - 8.1* partial, A.15.2.1
  - A.13.1.2
  - A.12.2.1

- Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, data transmission and references to detailed supporting and relevant business processes and technical measures implemented to enable:
  - A.10.8.2
  - A.11.4.6
  - A.11.6.1
  - A.12.3.1
  - A.12.5.4

- Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, data transmission and references to detailed supporting and relevant business processes and technical measures implemented to enable:
  - A.10.4.1
  - Commandment #4
  - Commandment #5
  - Commandment #1
  - Commandment #2
  - Commandment #3
  - Commandment #5
  - Commandment #11

- Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, data transmission and references to detailed supporting and relevant business processes and technical measures implemented to enable:
  - A.10.4.1
  - Commandment #4
  - Commandment #5
  - Commandment #1
  - Commandment #2
  - Commandment #3
  - Commandment #5
  - Commandment #11