ACCESS CONTROL POLICY COMPONENTS

Security Best-Practices
1 – Best-Practice Frameworks (NIST, SOC2)
2 – Standards

Legal Compliance
1 – Regulatory Requirements

Financial Governance
1 – Procurement Process
2 – Security Terms and Conditions
3 – Social Security & Financial Audits

Security Compliance
1 – SOC2 (SSAE-16) (Processes)
2 – PCI, SOX (Financial)
3 – HIPAA (Health)
4 – FISMA and FedRAMP (Government)

IT Controls
1 – Incidents (outages)
2 – Service Requests (change & modify)
3 – Change Management

Security Controls
1 – Segmentation, Zoning, and Ports (FWRR)
2 – Vulnerability Management (Patch/Pen)
3 – Configuration Hardening (Services/Settings)
4 – Security Agent Installs (AV/HIDS)

Reporting Controls
1 – Logging and Alerts (system access)
2 – Cloud Computing pricing alerts

Auditing Controls
1 – Logging and Alerts (system access)
2 – Cloud Computing pricing alerts
3 – Vendor Security Assessments

ACCESS CONTROL POLICY

Document Header

Table of Contents

Executive Summary

Access Roles
Data and Information Management

Account Types

Access Controls Processes
Account Management

Account Creation

Access Changes

Account Decommisioning

Account Audit and Logging
Access Validation

Information Governance

Appendix A : Terms and Definitions

Appendix B : References

Data and Information Controls
1 – Tracking Sensitive Data Types
2 – Connecting/Sharing Data Between Systems
3 – Cloud Geo-Data Centers Restrictions

Identity Management
1 – Use of credentials
2 – Application Platform Tagging
3 – Defining Non-User Access (API)
4 – Account Federation and Trusts

Access Management
1 – Tracking Internal and External User Access
2 – Restricting Privileged Accounts
3 – Password and MFA Access

Application Security
1 – Application Code Scanning (SCA/DCA)
2 – Code Versioning Controls
3 – Database/Storage Protection

Security Responsibilities
1 – Provider Responsibilities (IR/DR)
2 – Consumer Responsibilities (BC & IR)