POLICY VERWALTUNG ACCOUNT
final version V. 3

INHALT

POLICY VERWALTUNG ACCOUNT
final version V. 3

	DATUM	Vor- und Nachname	Rolle
Erstellung	10/04/07	Dr. Alessandro Bottonelli	Berater Symantec
Erstellung	16/05/07	Membri Gruppo ICTSEC Prov. Aut. di Bolzano	Mitarbeiter in der Erstellung
Revision		Ing. Fabio Battelli	Project Manager Symantec
Genehmigung		Dr. Simonetta Maina	Security Manager PAB
Revision	26/04/10	Sicherheitsdienst	Sicherheitsdienst
Genehmigung		Dr. Kurt Pöhl	Direktor der Abteilung Informationstechnik
Deutsche Version	26/11/2015	Ingrid Rimbl	

1. ZIEL UND EXECUTIVE SUMMARY

Ziel dieser Policy ist es die Sicherheitspolitik im Bereich der Erstellung von namentlichen Accounts für due Authentifizierung an den IT-System der Autonome Provinz Bozen (folgend APB oder Landesverwaltung) zu definieren.

Hauptziele einer korrekten Accountverwaltung sind:

- Einhaltung der Rechtsvorschriften (im Besonderen des Strafrechts und des Datenschutzkodex); für die Verwaltung der Administratorenaccounts (genäß der Definition der Verfügung der Datenschutzbehörde vom 27.11.2008) ist besonders die genannte Verfügung zu beachten.
- Die Sicherheit in der Verwaltung erhöhen, um zu gewährleisten, dass due einer natürlichen Person zugewiesenen Zugangsdaten auch nur von dieser Person genutzt werden und dass diese Zugangsdaten sofort

revidiert werden, sobald sie nicht mehr benötigt werden.;

- Vereinheitlichung der Verwaltung der Accounts in der Landesverwaltung;
- Vereinfachung der Verwaltung, soweit möglich, mit dem Zweck Größenvorteile zu erzielen, die Fähigkeit zur Kontrolle zu erhöhen und die Fehlerwahrscheinlichkeit in der Ausführung zu verringern.

2. ANWENDUNGSBEREICH

Dieses Dokument regelt die Verwaltung der Account (Zugangsdaten) die dem Zugang zu Ressourcen der IT , zu Informationen oder zum Netzwerk beinhalten. Sie gilt nicht für die Verwaltung von Administratorenaccounts.

3. VERWEISE

Vorliegendes Dokument verweist im Besonderen auf folgende Rechtsvorschriften:

- Gesetzesvertretendes Dekret Nr. 196/2003 (“Datenschutzkodex”) und Anlagen;
- Art. 615-ter des Strafgesetzbuches - Unerlaubter Zugang zu, durch Sicherheitsmaßnahmen geschützten telematischen Systemen (Accesso abusivo ad un Sistema Telematico protetto da misure di sicurezza);

auf folgende Dokumente der Landesverwaltung:

- Risikoanalyse 2005 pro-DPS (ex d.lgs.196/2003);

- Risikoanalyse 2006 pro-DPS (ex d.lgs.196/2003);
- Analyse Mindestmaßnahmen 2005 ex Anlage B d.lgs.196/2003;
- Analyse Mindestmaßnahmen 2006 ex Anlage B d.lgs.196/2003;
- Sicherheitsrichtlinien 2005 Abt.9;
- Policy Remotezugänge der Autonomen Provinz Bozen;

auf die Standards:

- ISO/IEC 27001 “Information Security Management System” (ex BS7799:2);
- ISO-TR13335 “Information Systems Security”;

und auf alle in der Industrie und allgemein international von Sicherheitsexperten angewandten Best-Practice-Regelungen, mit Besonderem Verweis auf die von der Forschungseinrichtung SANS Institute und von der Organisation ISC² kodifizierten Standards.

4. NAMENSGEBUNG

(vedi Allegato B)

5. VERANTWORTUNG

a) Der Sicherheitsdienst der Abt. 9 der Landesverwaltung ist Verantwortlich für die Erstellung, Genehmigung, Verteilung und Überarbeitung dieses Dokuments.

b) Jeder Bedienstete, Berater, Lieferant oder Mitarbeiter der Landesverwaltung, unabhängig vom Arbeitsverhältnis, der mit der Aufgabe betreut ist spezifische Prozeduren für die Erstellung von Accounts zu realisieren ist dafür verantwortlich, dass diese Prozeduren den Kriterien gegenständlichen Dokumentes entsprechen.

c) Jede Führungskraft der Landesverwaltung und jeder Datenschutzverantwortliche, auf Grund seiner Zuständigkeit, ist für die Überprüfung und Kontrolle verantwortlich, dass die Sicherheitskriterien, die dieses Dokument beschreibt, in Form und Inhalt von den Mitarbeitern unter seiner Verantwortung eingehalten werden.

6. AUSFÜHRUNG

6.1 Grundsätze

a) Rechtsinhaber der Daten, die Systeme und Datenbanken im Netz der Landesverwaltung verfügbar sind, ist die Autonome Provinz Bozen.

b) In der Regel haben folgenden Kategorien Anrecht auf einen Account für

den Zugang zu IT-Systemen der Landesverwaltung (natürliche Personen):

I) Bedienstete ;
II) Mitarbeiter;
III) Bedienstete, Berater und Mitarbeiter von Lieferanten;
IV) Bedienstete, Berater und Mitarbeiter von anderen konventionierten Körperschaften;

Eventuelle Ausnahmen werden vom Sicherheitsdienst der Abt. 9 beurteilt und vom Direktor der Abteilung 9 genehmigt.

c) Diese Policy muss gemäß Gesetzgebung auch ein angemessenes Sicherheitsniveau zum Schutz der als "vertraulich" angesehen Daten der Autonome Provinz Bozen und nicht nur der als "personenbezogenen" und/oder „sensible Daten" (gemäß gvD. 196/2003) klassifizierten Informationen gewährleisten

6.2 Organisatorische Vorraussetzungen

a) Vorraussetzungen für die Bediensteten der Landesverwaltung:

Kriterium	***Qualitative Bewertung***
Bediensteter der Landesverwaltung	Der "Arbeitgeber" ist der Abteilungsdirektor und daher ist es die Direktion der Abteilung, die die natürliche Person "identifiziert" und die Zugehörigkeit zur Landesverwaltung garantiert.
Rolle	Es muss ein Autorisierungssystem, technisch und organisatorisch, verfügbar gemacht werden, dass für homogene Klassen von Anwendern definiert ist, welche Aktionen erlaubt sind und auf welchen Daten.
Privacy	Enthält das System, auf dem der Zugang gewährt wird, personenbezogene Daten muss ein Beauftragungsschreiben erfolgen (AXAM).

b) Vorraussetzungen für die Mitarbeiter der Landesverwaltung:

Kriterium	***Qualitative Bewertung***
Mitarbeiter der Landesverwaltung	Der "Arbeitgeber" ist der Abteilungsdirektor und daher ist es die Direktion der Abteilung, die die natürliche Person "identifiziert".
Zeitliche Begrenzung	Die Abteilung, die den Vertrag mit dem Mitarbeiter verwaltet, muss festlegen BIS WANN dieser Vertrag gültig ist: Datum oder „unbefristet" - letzteres aus rechtlichten Gründen selten
Rolle	Es muss ein Autorisierungssystem, technisch und organisatorisch, verfügbar gemacht werden, dass für homogene Klassen von Anwendern definiert ist, welche Aktionen erlaubt sind und auf welchen Daten.
Privacy	Enthält das System, auf dem der Zugang gewährt wird, personenbezogene Daten muss ein Beauftragungsschreiben für einen externen Beauftragten erfolgen (AXAM).

c) Requisiti per dipendenti, consulenti e collaboratori di fornitori in outsourcing (se accesso remoto, vedi anche "Policy Accesso Remoto"):

Kriterium	***Qualitative Bewertung***
Bediensteter eines Unternehmens	Der Lieferant hat ein laufendes kommerzielles Verhältnis mit der APB (Dienstleistungsvertrag)
Berater der Landesverwaltung	Die Abteilung, die den Vertrag mit dem Berater verwaltet, identifiziert die natürliche oder juristische Person und garantiert für den

Kriterium	***Qualitative Bewertung***
	Beratungsvertrag.
Zeitliche Begrenzung	Die Abteilung, die den Vertrag mit dem Berater/Lieferant verwaltet, muss festlegen BIS WANN dieser Vertrag gültig ist: Datum oder „unbefristet“ - letzteres aus rechtlichten Gründen selten
Rolle	Es muss ein Autorisierungssystem, technisch und organisatorisch, verfügbar gemacht werden, dass für homogene Klassen von Anwendern definiert ist, welche Aktionen erlaubt sind und auf welchen Daten.
Privacy	Ernennung seitens der APB zum externen Verantwortlichen für die Datenverarbeitung und Erklärung des Lieferanten der Einhaltung des Datenschutzkodex. Dem Lieferant obliegt die Beauftragung seine Mitarbeiter mit eigenen Kriterien und Mittel.
Sicherheit	Erklärung des Lieferanten der Einhaltung der Sicherheitsvorgaben gemäße Gesetzgebung, Regelung oder Vertrag (gvD.196/2003, Zivilgesetzbuch, Strafgesetzbuch und allen anderen anzuwenden Vorschriften auf Grund der verarbeiteten Daten)

d) Requisiti per dipendenti, consulenti e collaboratori di altri Enti:

Kriterium	***Qualitative Bewertung***
Bediensteter einer Körperschaft	Die Körperschaft hat ein gültiges Übereinkommen mit der APB
Rolle	Es muss ein Autorisierungssystem, technisch und organisatorisch, verfügbar gemacht werden, dass für homogene Klassen von Anwendern definiert ist, welche Aktionen erlaubt sind und auf welchen Daten.
Privacy	Die Körperschaft ernennt die eigenen Mitarbeiter zu Beauftragten mit eigenen Kriterien und Mitteln.
Sicherheit	Erklärung der Körperschaft der Einhaltung der Sicherheitsvorgaben gemäße Gesetzgebung, Regelung oder Vertrag (gvD.196/2003, Zivilgesetzbuch, Strafgesetzbuch und allen anderen anzuwenden Vorschriften auf Grund der verarbeiteten Daten)

6.3 Vorraussetzungen

Vorwort

Die hier angeführten Vorraussetzungen geben nicht die Modalitäten an, mit denen diese realisiert werden. Die Lösungen können sowohl technisch als auch verwaltungstechnisch umgesetzt werden. Die Wahl der geeignetsten Lösung ist Entscheidung der für die Tätigkeiten verantwortlichen Person/Struktur. In diesem Sinne ist mit der Anweisung in diesem Dokument „Erstellen einer Prozedur“ nicht die Erstellung einer technischen Prozedur (Automatismus) gemeint oder wie eine „verwaltungstechnische/organisatorische Prozedur zu erstellen“ ist.

Welche Lösung auch immer gewählt wird – technisch oder organisatorisch – ist die Dokumentation zur Darlegung der Tätigkeiten unabdingbar.
Die im Folgenden angeführten Punkte beziehen sich auf die Verwaltung der Accounts, die dem Zugang zu IT-Systemen und zu Informationssystemen der Autonomen Provinz Bozen dienen.

(1) Jedem Account auf Systemen der APB (dem mindesten ein Zugang – Benutzername und Kennwort – entspricht) muss einer und ausschließlich einer klar identifizierten natürlichen Person zugeordnet sein

(2) Sofern nötig, ist es möglich derselben natürlichen Person mehrere Zugangsdaten zu übergeben. Die Zugangsdaten werden immer in getrennten Kanälen mitgeteilt (z.B. Benutzername via Mail und Kennwort mündlich oder via SMS)

(3) Die natürliche Person muss immer “identifiziert” werden, bevor ihr ein Account zugeordnet werden darf, daher muss vor Übergabe der Zugangsdaten, die den Zugang zu einer oder mehrere IT-Ressourcen, zu Informationen oder zum Netzwerk der APB erlaubt, die Identität geklärt sein. Diese Identifizierung ist Aufgabe des „Arbeitgebers“ (in der Regel der Abteilungsdirektor) der natürlichen Person.

(4) Der Account und die entsprechenden Daten zur Authentifizierung, sofort

nach der ersten Anwendung und der damit verbunden zwingenden Änderung seitens des Nutzers , darf der geheimen Teil der Zugangsdaten (Kennwort oder PIN im Falle von Smart-cards oder Token oder biometrischer Systeme) nur der natürlichen Person der die Zugangsdaten zugewiesen wurden bekannt sein.

(5) Erstellen einer Prozedur die garantiert, soweit technisch möglich, dass de die Systeme so konfiguriert sind, dass mindestens folgendes wahr ist:

- Mindestlänge des Kennwortes entspricht acht Zeichen;
- Das Kennwort enthält sowohl Buchstaben als auch Ziffern (mindestens zwei Ziffern), aber keine Sonderzeichen, wie Umlaute, Akzente oder ähnliches (gemäß ISO-9660: von a-z, A-Z, 0-9). Sonderzeichen wie beispielsweise :$, %, &, ;, und ähnliche, ist eine Überprüfung der Handhabung in Gange.
- Es empfiehlt sich außerdem, sofern technisch möglich, banale Kennwörter nicht zu akzeptieren. Zum Beispiel:
  - ✓ Übereinstimmung mit dem Benutzernamen auch wenn Ziffern oder Buchstaben vor- oder nachgestellt werden;
  - ✓ Aus Wörterbüchern (Städtenamen, Eigennamen, u.s.w. einbegriffen);
  - ✓ Mehr als zweifache (dreifach, vierfach, u.s.w. etc.) Wiederholung desselben Zeichens in Folge;

Für Systeme, die als kritisch betrachtet werden, können diese Maßnahmen weiterführend bewertet werden

(6) Erstellen einer Prozedur, die gewährleistet, dass die Systeme soweit technisch möglich so konfiguriert sind, dass der Nutzer gezwungen ist, das Kennwort nach drei Monaten zu ändern und dass die letzte fünf verwendeten Kennwörter nicht akzeptiert werden. Dort wo dies technisch nicht umsetzbar ist, muss die organisatorisch geregelt werden, unter Anweisung der Anwender.

(7) Die Prozeduren für die Erstellung, die Verwaltung, und den Widerruf der Accounts muss gewährleiseten, dass der einer natürlichen Person zugewiesene Benutzername innerhalb eines “System” einzig ist (wobei unter System je nach Kontext eine Datenbank, ein Active Directory Forest, ein einzelnes System mit lokaler Authentifizierung zu verstehen ist).

(8) Die Prozeduren für die Erstellung, die Verwaltung, und den Widerruf der Accounts muss gewährleiseten, dass der einer natürlichen Person zugewiesene Benutzername nicht einer andere natürlichen Person innerhalb eines "System" zugewiesen wird(wobei unter System je nach Kontext eine Datenbank, ein Active Directory Forest, ein einzelnes System mit lokaler Authentifizierung zu verstehen ist).

Um zu gewährleisten, dass die Vorgaben in Punkt 7 und 8 eingehalten werden , ist es empfehlenswert für die Benutzernamen eine einzige Konvention zu vereinbaren, damit innerhalb eines "Systems" Gleichnamigkeiten zu vermieden werden

(9) Um zu gewährleisten, dass derselbe Benutzername nicht verschiedenen natürlichen Personen zu verschiedenen Zeitpunkten zugewiesen wird und um eine Historisierung der Zuordnung von Benutzername und natürlicher Person zu erstellen:

- ✓ Accounts deaktivieren anstatt sie zu löschen wenn er nicht mehr benötigt wird. So verhindert das System automatisch, die Wiederverwendung eines Benutzernamens;

- ✓ Ein Verzeichnis mit folgenden Informationen führen:

  Welchen natürlichen Personen wurden Benutzernamen zugewiesen,
  Datum der Aktivierung,
  Datum der Deaktivierung.

  Dies erlaubt es, sofern notwendig, mit Sicherheit zu überprüfen welcher Username welcher natürlichen Person zugeordnet wurde.

(10) Erstellen einer Prozedur, wenn technisch möglich durch eine Automatisierung unterstützt, die mit mindestens wöchentlich, seit mehr als 180 Tagen „schlafende" Accounts (nicht genutzte) ermittelt.

(11) Erlaubt das System keine automatische Überprüfung in Bezug auf Punkt (10), muss diese Kontrolle manuell durch den Systemadministrator erfolgen. In diesem Fall erfolgt dies mindestens

monatlich. Es müssen in diesem Fall Accounts die seit mehr als 150 Tagen nicht genutzt werden , ermittelt werden

(12) Die Liste eventueller schlafender Accounts ist dem „Arbeitgeber“ (in der Regel der Abteilungsdirektor) oder einer entsprechenden Figur vorzulegen, damit eine Begründung für die Nichtnutzung und die eventuelle Deaktivierung des Account verifiziert werden kann (eventuelle Fehler oder begründete Inaktivität wegen Wartestand o.ä.)

(13) Erstellen einer Prozedur, die beschreibt wie und mit welchen Mitteln der „Arbeitgeber“ (in der Regel der Abteilungsdirektor) oder einer entsprechenden Figur, den Systemadministrator sofort über Änderungen der Zuständigkeit des Bediensteten, des Beraters oder Mitarbeiters informiert.

(14) Erstellen einer Prozedur, die garantiert, dass der Systemadministrator sofort Accounts bei Dienstaustritt oder weil der Zugang nicht mehr nötig ist, deaktiviert (nicht löscht, siehe Punkt 9) wenn der Inhaber des Accounst

(15) Konfiguration der Terminals und Arbeitsplätze, wo technisch machbar, mit einem durch ein Kennwort geschütztem Bildschirmschoner (screensaver), der sich nach 10 Minuten Pause aktiviert.

(16) Innerhalb der Organisation der Landesverwaltung existieren mehrere Benutzeraccounts für mehrere Beauftragte mit verschieden Zugangsprivilegien zum System. Deshalb ist ein Autorisierungungssystem ("Sistema di Autorizzazione"), gemäß Punkt 12 der Anlage B des gvD. 196/2003 und den Vorgaben für den Rechtsinhaber und/oder Verantwortlichen für die Verarbeitung der Vorschrift der Datenschutzbehörde vom 27/11/2008 verpflichtend:

- ✓ Erstellen einer Prozedur zur Identifikation und Führung eines Registers der Rollen (und der ihnen zugeordneten Systemprivilegien) bevor mit der der Verarbeitung und der Vergabe von Zugangsrechten auf personenbezogenen Daten begonnen wird.

- ✓ Für jeden Beauftragen oder Typologie von Beauftragten sind die Berechtigungsprofile notwendig und ausreichend für die Abwicklung der beauftragten Verarbeitungen. Dies geschieht nominell oder für Klassen von Beauftragten, Klassen die normalerweise mit dem zugehörigen Amt und/oder Arbeitsauftrag (Rolle) des Beauftragten übereinstimmen

- ✓ Regelmäßige Übrprüfung, mindestens ein Mal pro Jahr, dass die Berechtigungen der Anwender noch gültig sind und frühzeitige Mitteilung eventueller Änderungen an die Systemadministratoren mit entsprechenden Maßnahmen. Es obliegt dem Systemadministratore die Berechtigungsprofile auf das System im Falle von Änderungen, anzupassen.

- ✓ Erstellen einer Prozedur zur Identifikation und Führung eines Register der Verwalter des IT-System und der zugordneten Rechte. Überprüfung durch den Verantwortlichen der Verarbeitung (Arbeitgeber), mindestens ein Mal pro Jahr, dass die Berechtigungen der Anwender noch gültig sind und frühzeitige Mitteilung eventueller Änderungen an die Systemadministratoren mit entsprechenden Maßnahmen. Es obliegt dem Systemadministratore die Berechtigungsprofile auf das System im Falle von Änderungen, anzupassen.

(17) Die natürliche Person der ein Benutzeraccount zugeordent ist(die also im Besitz von Benutzrnamen und Kennwort ist) muss(*) über die eigenen Pflichten und Verantwortungen informiert sein:

- Das Kennwort gemei halten (oder der PIN im Falle von Zugängen über smart-card, token oder biometrische Systeme);
- Sofortige Mitteilung eines effektiven oder vermutlichen Verlustes, Zerstörung oder Verbreitung von Kennwort, PIN, smart-card oder token;
- Die eigenen Kennwörter (oder PIN) nicht auf Notizzetteln oder anderen leicht zugänglichen Träger festhalten.

(18) Die Beauftragen darüber informieren(*), durch eine Vertragsklausel oder andere anwendbare vergleichbare Mittel, sich vom Arbeitsplatz ab zu melden (Logoff) wenn er sich von demselebne entfernt, mindestens innerhalb des Arbeitstages.

(*) die Umsetzung wird vom Sicherheitsdienst der Abt. 9 und dem Organisationsamt überprüft;

(19) Systemadministratoren, DBA und Verwalter müssen spezifische Benutzeraccounts für ihre Arbeit in der Verwaltung/Instandhaltung verwenden. Für diese Benutzeraccounts gelten die Vorgaben der Vorschrift der Datenschutzbehörde vom 27/11/2008.

(20) Eventuelle personenbezogene Daten die veröfentlicht werden (z.B. web SEiten des öffentlichen Portals der Landesverwaltung) können von den Sicherheitsmaßnahmen des Berechtigungssystems und den Maßnamen zur Sicherheit des Systems ausgenommen werden.

VORLAGE A

Fac-simile für die Mitteilung von Anmerkungen in Bezug auf die relative alla Policy Verwaltung Account

Abteilung APB	Abt.__ . __
GESEHEN VOM VERANTWORTLICHEN	_____ am ___ / ___ / _____
ABSENDER	Name _____Nachmame _____ Email _____
DATUM	__ / __ / _____
ART DER ANMERKUNG	( ) Formaler Fehler im Dokument ( ) Potenzielle Kritizität ( ) Mögliche Verbesserung ( ) Anderes (angeben): _____
ABSATZ UND BUCHSTABE	§ ___ Punkt ____ (N.A. angeben sofern nicht anwendbar)
ANMERKUNG	