Dienstvereinbarung

über den Einsatz von Firewallsystemen an der Freien Universität Berlin

gemäß § 74 Personalvertretungsgesetz Berlin (PersVG) in der aktuellen Fassung und in Ergänzung des Tarifvertrages über die Arbeitsbedingungen von Arbeitnehmern auf Arbeitsplätzen mit Geräten der Informationstechnik (Tarifvertrag Infotechnik) in der aktuellen Fassung wird zwischen der Leitung der Freien Universität Berlin und dem Gesamtpersonalrat der Freien Universität Berlin nachstehende Dienstvereinbarung über den Einsatz von Firewallsystemen geschlossen.

§ 1 Allgemeiner Grundsatz

Die Dienstvereinbarung gilt ergänzend zu sonstigen an der Freien Universität Berlin geltenden Regelungen und Vorschriften über die Nutzung von Informationstechnik, insbesondere der "Rahmendienstvereinbarung über die Einführung und Anwendung Daten verarbeitender Systeme an der Freien Universität Berlin".

§ 2 Gegenstand und Geltungsbereich

Gegenstand der Dienstvereinbarung ist der Betrieb von Firewallsystemen an der Freien Universität Berlin. Unter einer Firewall ist ein organisatorisches und technisches Konzept zur Trennung und Abschirmung von Netzbereichen aus Gründen der IT-Sicherheit zu verstehen. Als Schnittstelle zwischen einzelnen Netzen, kontrolliert die Firewall den Netzwerkverkehr zwischen den Netzen, um ungewünschten Verkehr zu verhindern und nur bestimmte, im Vorfeld definierte Zugriffe zu gestatten. Zu den zentralen Aufgaben von Firewallsystemen gehören zum einen die Reglementierung von Kommunikationsbeziehungen zwischen unterschiedlichen Schutzniveaus (Beschränkung von Netzdiensten) und zum anderen die Überwachung der ausgetauschten Daten (Protokollierung und Analyse des Datenverkehrs).

§ 3 Zweckbestimmung

Die Dienstvereinbarung hat den Zweck, die Verfahren der Protokollierung bei dem Betrieb von Firewallsystemen sowie die Kontrolle und Auswertung dieser Protokolle verbindlich zu regeln.

§ 4 Änderungen des Regelwerks

1. Jede Änderung am Regelwerk der Firewalls darf nur auf Antrag erfolgen. Der Antrag bedarf der Schriftform, wobei auch die elektronische Form durch Verwendung von E-Mails, benutzt werden kann. Es ist nicht erforderlich, dass eine E-Mail mit einer digitalen Signatur gemäß dem deutschen Signaturgesetz unterschrieben wird. Die Details und der Umfang der einzelnen Angaben sind in der Verfahrensbeschreibung zum IT-Verfahren "Zentrale Sicherheitsinfrastruktur" festgelegt.
2. Ein Antrag auf Änderung des Regelwerks muss an den Verfahrensverantwortlichen des IT-Verfahrens "Zentrale Sicherheitsinfrastruktur" gerichtet werden. Der Verfahrensverantwortliche entscheidet im Allgemeinen über die Durchführung der beantragten Änderung des Regelwerks durch die zugriffsberechtigten Personen.
3. In strittigen Fällen, in denen der Verfahrensverantwortliche und der Antragsteller über eine Lösung bezüglich einer Änderung des Regelwerks keine Einigung erzielen können, wird der Vorgang an eAS-IT-S eskaliert. In diesem Fall leitet der Verfahrensverantwortliche diesen Antrag zusammen mit einer kurzen Einschätzung, inwieweit die Sicherheit des Firewall-Systems durch die gewünschte Änderung beeinflusst wird, an eAS-IT-S zur Entscheidung weiter.
4. In begründeten Notfällen kann der Antrag auch mündlich gestellt werden. Wenn der Verfahrensverantwortliche keine wesentliche Beeinträchtigung der Sicherheit feststellt, kann die gewünschte Änderung vorläufig sofort vorgenommen werden. Der Antragsteller muss in diesem Fall so schnell wie möglich den Antrag in Schriftform nachreichen.
5. In bestimmten Ausnahmefällen kann für einen festgelegten Zeitraum die mündliche Antragstellung zwischen dem Verfahrenverantwortlichen der Zentralen Sicherheitsinfrastruktur und dem Antragsteller vereinbart werden. Die Vereinbarung über den festgelegten Zeitraum muss unter Angabe der Gründe schriftlich dokumentiert und der Personalvertretung bekannt gegeben werden. Wenn innerhalb von drei Tagen nach Bekanntgabe die Personalvertretung nicht widerspricht, gilt die Vereinbarung als zugestimmt.

§ 5 Protokollierung und Auswertung

1. Kommunikation, die das Regelwerk der Firewall zulässt, wird nicht protokolliert.
2. Unzulässige Zugriffsversuche werden einer automatischen, systembedingten Protokollierung der sicherheitsrelevanten Vorgänge unterzogen. Die Protokolle werden dabei ausschließlich zu Zwecken

- der Gewährleistung der Systemsicherheit, insbesondere der Sicherung der zu schützenden Netze vor unbefugten Zugriffen bzw. unbefugter Kommunikation,
- der Analyse und Korrektur technischer Fehler,
- der technischen Optimierung des Netzes und der im Netz angebotenen Dienste (optimale Kapazitätsauslegung, angemessene Wartezeiten) sowie
- der Aufklärung missbräuchlicher Nutzung der Internetdienste gemäß den in der IT-Rahmendienstvereinbarung festgelegten Regelungen

verwendet.

3. Der Zugriff auf Protokolle ist auf die mit der technischen Administration des Systems betrauten Personen beschränkt und darf nur im Rahmen der ihnen obliegenden Aufgaben (System- und Netzsicherheit, Korrektur technischer Fehler) erfolgen.
4. Sofern Protokoll- und Verbindungsdaten mit einem Personenbezug zu Beschäftigten nicht länger für eine zulässige Verarbeitung erforderlich sind, müssen diese unverzüglich, spätestens jedoch nach drei Monaten, gelöscht werden.

§ 6. Zugriffsberechtigungen

1. Die Zugriffsberechtigungen mit Systemprivilegien zu den Programmen und Daten im Zusammenhang mit dem Betrieb von Firewallsystemen werden organisatorisch und programmtechnisch geregelt. Die Zugriffsberechtigungen sind möglichst eng zu fassen.
2. Weisungen vorgesetzter Stellen an Administratoren, die Auswertungen der Protokolldaten außerhalb der in dieser Dienstvereinbarung definierten Zwecke zum Inhalt haben, sind unzulässig.

§ 7 Schlussbestimmungen

1. Die Dienstvereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden. Im Falle einer Kündigung der Dienstvereinbarung verpflichten sich die Vertragsparteien unverzüglich in Verhandlungen über eine neue Dienstvereinbarung einzutreten.
2. Bis zum Abschluss einer neuen Vereinbarung gilt diese Vereinbarung weiter.

3. Im Zusammenhang mit dieser Dienstvereinbarung gelten auch die Regelungen der "Rahmendienstvereinbarung über die Einführung und Anwendung Daten verarbeitender Systeme an der Freien Universität Berlin", abgeschlossen am 04.07.2006. Sofern diese Dienstvereinbarung vom 04.07.2006 gekündigt werden sollte, gelten ihre Regelungen im Bezug auf die vorliegende Dienstvereinbarung "über den Einsatz von Firewallsystemen an der Freien Universität Berlin" in Nachwirkung so lange weiter, bis die IT-Rahmendienstvereinbarung vom 04.07.2006 durch eine andere Dienstvereinbarung ersetzt worden ist.

Berlin, den 31.10.06

Peter Lange
Kanzler (mdWb)

Petra Botschafter
Vorsitzende des GPR

Anhang

1.1 Antragsformular zur Änderung am Regelwerk der Firewall-Systeme

Beantragende Stelle

Name und Anschrift des Fachbereichs /Zentrale Einrichtung/Institut/Abteilung:	
Name des IT-Verantwortlichen:	
Ansprechpartner (Name, Tel.-Nr., E-Mail-Adresse):	

Angaben zur Kommunikationsverbindung:

Lfd. Nr.	**Quelle** (IP-Adresse / Rechnername)	**Ziel** (IP-Adresse / Rechnername)	**Protokoll** (ggf. Port-Nr.)	**Dienst** (ggf. Port-Nr.)
1				
2				
3				

Hinweis: Bei Bedarf kann die Tabelle erweitert werden.

Zeitangaben:

□ Die Kommunikationsverbindungen sollen dauerhaft eingerichtet werden.

□ Die Kommunikationsverbindungen sollen von bis eingerichtet werden.

Ggf. Zeitfenster:

Die Kommunikationsverbindung muss an den Wochentagen zur Verfügung stehen:

□ alle Wochentage □ Montag bis Freitag □ folgende Wochentage:

.....

.....

.....

Die Kommunikationsverbindung muss zu folgenden Uhrzeiten zur Verfügung stehen:

.....

.....

.....

Bitte begründen Sie die Notwendigkeit der gewünschten Kommunikationsverbindung/en:

Berlin, den

Unterschrift des Antragstellers	Unterschrift des IT-Verantwortlichen

1.2 Antrag zur befristeten Ausnahme von der schriftlichen Antragspflicht bei Regeländerungen

Beantragende Stelle

Name und Anschrift des Fachbereichs /Zentrale Einrichtung/Institut/Abteilung:	
Name des IT-Verantwortlichen:	
Ansprechpartner (Name, Tel.-Nr., E-Mail-Adresse):	

Zeitraum, in dem die Pflicht zur schriftlichen Antragstellung auf Änderung am Regelwerk der zentralen Firewallsysteme entfällt:

Begründung:

Berlin, den

Unterschrift des Antragstellers

Unterschrift des Verfahrensverantwortlichen „Zentrale Sicherheitsinfrastruktur“