HSG-IT-Benützungsvorschriften

vom 1. März 2016[1] (Stand 15. Mai 2018)

Der Senatsausschuss erlässt

gestützt auf Art. 35 Abs. 2 des Universitätsstatuts vom 25. Oktober 2010[2]

als Benützungsvorschriften:

Präambel

Die tägliche Arbeit in Lehre, Forschung, Weiterbildung und Beratung an der Universität St.Gallen (HSG) stützt sich immer stärker auf Informations- und Kommunikationstechnologien (IT) ab. Die Nutzung der von der für die Informatik zuständigen Stelle (kurz: zentrale IT) erbrachten IT-Dienstleistungen unterliegt verschiedenen rechtlichen und organisatorischen Rahmenbedingungen, deren Einhaltung für den sicheren, stabilen und effizienten IT Betrieb an der HSG unverzichtbar ist. Die folgenden HSG-IT-Benützungsvorschriften fassen entsprechende Regelungen zusammen.[3]

1 Zugangsberechtigung zu den Systemen[4]

HSG-Angehörige erhalten nach der Immatrikulation (Studierende) oder bei ihrer Anstellung (Angestellte) für den Zugang zum Netzwerk der HSG (HSGnet) einen HSG-Benutzernamen und ein dazu gehöriges HSG-Passwort.

Nicht-HSG-Angehörigen (3rd Level Supporter/Administratoren, Gäste) kann auf Antrag an die zentrale IT, welcher durch den IT-Administrator der Organisationseinheiten zu stellen ist, ebenfalls ein HSG-Benutzername erteilt werden. Der Zugang zu den IT-Systemen der HSG kann inhaltlich und/ oder zeitlich limitiert werden. Für unterschiedliche Dienste können unterschiedliche HSG-Benutzernamen und -Passwörter vergeben werden.

Die Zugangsberechtigung zum HSGnet erlischt mit der Exmatrikulation (Studierende), der Auflösung des Arbeitsverhältnisses (Angestellte), dem Wegfall des Grundes für den Zugang (Nicht-HSG-Angehörige) oder nach Ende der Gültigkeitsdauer (zeitlich befristete Berechtigungen). Sonderregelungen z.B. für emeritierte Professorinnen und Professoren bleiben vorbehalten.

2 Hardware

2.1 HSG-Geräte

Erfolgt die Finanzierung eines IT-Arbeitsplatzes durch die Kernuniversität oder ein Institut, stellt die zentrale IT entsprechende HSG-Endgeräte (Desktops, Laptops, …) bereit. Die jeweils verfügbaren Endgeräte ergeben sich aus der separaten Regelung betr. IT-Arbeitsplätzen an der HSG.

---

[1] Nachgetragen durch Beschluss des Senatsausschusses vom 15. Mai 2018.
[2] sGS 217.15
[3] Ergänzende und detailliertere Regelungen und Weisungen bezüglich der Nutzung von IT Dienstleistungen sind im HSG Intranet abgelegt.
[4] Nachgetragen durch Beschluss des Senatsausschusses vom 15. Mai 2018; Inkraftsetzung per 15. Mai 2018.

Jede Mitarbeiterin und jeder Mitarbeiter ist verpflichtet, sorgsam mit ihren Geräten umzugehen. Die Sorgfaltspflicht beinhaltet nebst der Vermeidung von physischen Schäden am Gerät insbesondere auch das Beachten der sicherheitsrelevanten Kriterien gemäss Ziff. 3.9.
HSG-Geräte müssen nach Beendigung des Arbeitsverhältnisses an die zentrale IT zurückgegeben werden.

2.2 Private Geräte und nicht von der zentralen IT betriebene IT-Infrastruktur

Externe oder interne Zugriffe mit privaten Endgeräten auf das Netzwerk der HSG können den ordnungsgemässen Betrieb des Netzwerks gefährden. Deshalb ist insbesondere darauf zu achten, dass solche Geräte stets über einen aktualisierten Virenschutz und ein aktualisiertes Betriebssystem verfügen.

Die zentrale IT berät die Mitarbeitenden der Institute und der Verwaltung in Fragen des Virenschutzes und der Aktualisierung von Geräte-Betriebssystemen. Es bleibt der zentralen IT vorbehalten, den externen Zugriff auf kritische Ressourcen des Netzwerks der HSG mit technischen Mitteln einzuschränken.

Folgende Punkte sind ebenfalls zu beachten:

a. Der Betrieb kommunikationsfähiger Endgeräte in den geschützten Netzwerkbereichen der HSG ist grundsätzlich der zentralen IT vorbehalten. Der Betrieb eines privaten kommunikationsfähigen Endgeräts in einem geschützten Netzwerkbereich kann über den zuständigen IT-Administrator bei der zentralen IT beantragt werden.
b. Externe stationäre Netzwerkverbindungen über andere als die von der zentralen IT zur Verfügung gestellten Kanäle sind unzulässig.
c. Der Betrieb von WLAN Access Points ist innerhalb des gesamten HSG-Netzwerks ausschliesslich Sache der zentralen IT.
d. Der Betrieb von Servern ist grundsätzlich Sache der zentralen IT. In begründeten Ausnahmefällen ist der Betrieb von Servern durch Organisationseinheiten der HSG ausnahmsweise zulässig. Die zentrale IT definiert die einzuhaltenden Mindestanforderungen. Die Bewilligungen werden gegen schriftlichen Nachweis der eingehaltenen Mindestanforderungen durch den Leiter der zentralen IT gewährt.
e. Die zentrale IT ist befugt, Server und andere kommunikationsfähige Endgeräte vom Netzwerk zu trennen, sofern das Netzwerk durch deren Betrieb gestört wird oder falls Gefahr in Verzug ist.

2.3 Diebstahl und Verlust

Der Versicherungsschutz für ein Endgerät im Eigentum der HSG ist durch die Universität gewährleistet. Versichert sind unvorhergesehen und plötzlich eintretende Beschädigungen oder Zerstörungen als Folge äusserer Einwirkung sowie Diebstahl. Nicht versichert sind Schäden aufgrund kriegerischer Ereignisse, Terrorismus etc. In jedem Fall nicht versichert sind Mobiltelefone bzw. Smartphones. Pro Schadenfall gilt ein Selbstbehalt.

3 Daten und Informationen

3.1 Software

Die von der HSG lizenzierte Software wird zentral auf die Hardware der HSG aufgespielt. Bei Verwendung nicht von der HSG lizenzierter Software hat die Benutzerin oder der Benutzer für die entsprechende Lizenzierung zu sorgen.

Die private Nutzung der Software ist im Rahmen der jeweiligen Lizenzbestimmungen möglich. Software, die auf einem privaten und nicht durch die zentrale IT zur Verfügung gestellten Gerät installiert wurde, muss – sofern eine weitere Nutzung nicht ausdrücklich erlaubt wurde – nach der Exmatrikulation bzw. nach Ende des Dienstverhältnisses dauerhaft vom Gerät gelöscht werden.

Die zentrale IT berät die Mitarbeitenden der Institute und der Verwaltung in Fragen zur Lizenzierung von Software.

3.2 Inhalt und Verbreitung von Informationen

Inhalte, Nachrichten und Mitteilungen, die über die IT-Infrastruktur der HSG übermittelt werden oder auf den IT-Systemen der HSG gespeichert werden, dürfen nicht gegen gesetzliche Bestimmungen verstossen. Ergänzende Vorgaben der HSG sind einzuhalten.

Zu beachten sind insbesondere Einschränkungen und Verbote, wie sie sich aus dem Strafgesetzbuch (SR 311.0) sowie den Bestimmungen über den Datenschutz (insbes. Datenschutzgesetz, SR 235.1 und sGS 142.1) und den Persönlichkeitsschutz (insbes. Art. 28 ZGB, SR 210) ergeben.

Die Benutzerinnen und Benutzer sind verantwortlich für die von ihnen übermittelten und gespeicherten Inhalte. Sie haben Ansprüche Dritter, welche auf missbräuchlicher Nutzung des HSGnet beruhen, selbst zu tragen. Sollte die Universität oder der Kanton St.Gallen daraus in Anspruch genommen werden, so steht ihnen der Rückgriff auf die Verursacherin oder den Verursacher zu. Sie können ihr oder ihm im Sinne des Gesetzes über die Zivilrechtspflege den Streit verkünden.

3.3 Webauftritt

Der Webauftritt der HSG gliedert sich in einen öffentlich zugänglichen Teil, dem Internetauftritt, und einen nichtöffentlichen Teil, dem Intranetauftritt.

Für die graphische Gestaltung des Webauftritts der HSG und ihrer Organisationseinheiten ist das für Belange der Kommunikation zuständige Ressort zuständig. Es erlässt dafür entsprechende gestalterische Vorgaben bzw. Empfehlungen. Die inhaltliche Verantwortung für den Webauftritt teilen sich von den Organisationseinheiten der HSG benannte Content Verantwortliche.

Die Verbreitung von HSG-internen Informationen, die allgemeinen Charakter haben bzw. sich an einen grösseren Benutzerkreis richten, erfolgt ausschliesslich über den Intranetauftritt. Im Intranet- und im Internetauftritt der HSG ist zu beachten, dass keine Urheberrechte verletzt werden, beispielsweise durch das Verwenden von nicht lizenzierten oder nicht frei verwendbaren Fotos.

3.4 Social Media

Bei der geschäftlichen Nutzung der von der HSG offiziell verwendeten Social Media Plattformen sind die universitätsinternen Vorgaben zu beachten.

3.5 Massenmail

Als Massenmail wird der einmalige Versand gleichlautender Mails an einen unbestimmten internen oder/und externen Empfängerkreis bezeichnet. Dabei ist es unerheblich, ob die Mails in mehreren Tranchen oder als Gesamtheit verschickt werden.

Der Versand von Massenmails muss beim Generalsekretariat beantragt werden, welches sich dabei an der geltenden Anti-Spam-Gesetzgebung orientiert.

3.6 Rechte Dritter

Bei der Nutzung der IT-Systeme der HSG, insbesondere der Web- und Kollaborationsplattformen, sind die Rechte Dritter, wie sie sich namentlich aus dem Persönlichkeitsschutz sowie der Gesetzgebung über das Urheberrecht und den Datenschutz ergeben, zu beachten.

Urheberrechtlich geschütztes Material darf ohne Genehmigung der Rechteinhaberinnen oder der Rechteinhaber auf IT-Systemen der HSG nicht verfügbar gemacht werden.

Benutzerinnen und Benutzer haben im Rahmen der geltenden gesetzlichen Bestimmungen das Recht, in allgemein zugänglichen Bereichen der IT-Systeme der HSG (z.B. Intranetauftritt, Internetauftritt, Kollaborationsplattformen etc.) abgelegte urheberrechtlich geschützte Materialien für den Eigengebrauch zu kopieren (vgl. Art. 19 und 20 des Urheberrechtsgesetzes, SR 231.1). Die Weiterverteilung auch auf nichtkommerzieller Basis ist nur mit Zustimmung der Rechteinhaberinnen oder der Rechteinhaber erlaubt. Sofern Benützungs- und Lizenzbestimmungen vorliegen, sind diese auf jeden Fall einzuhalten.

3.7 Veränderung von Informationen

Die für Kommunikations-, Studierenden- und Personalbelange zuständigen Ressorts sowie die zentrale IT sorgen für eine minimale Ordnung in jenen Bereichen, die allen Benutzerinnen und Benutzern zugänglich sind (namentlich Intranetauftritt, Internetauftritt und offizielle Social Media Kanäle). Sie sind dabei berechtigt, die veröffentlichten Inhalte entweder mit Einwilligung der Erstellerin oder des Erstellers zu verändern oder aber die Inhalte zu löschen – unabhängig davon, ob sie den Anforderungen an den Inhalt von Informationen gemäss Punkt 3.2 genügen oder nicht. Dies betrifft namentlich auch die für den Datenaustausch gedachten Speicherorte, auf denen Dateien ohne Rückfrage nach einer bestimmten Zeitdauer gelöscht werden.

3.8 Datenablage[5]

Geschäftsdaten und nicht-öffentliche Forschungsdaten sind grundsätzlich an offiziellen Ablageorten der HSG[6] abzulegen, vorbehaltlich abweichender vertraglicher Vereinbarungen. Damit wird die Verfügbarkeit und Sicherheit der Daten gewährleistet. Die Benutzer tragen dabei Sorge, dass die Daten an Orten mit entsprechend definierten Zugriffsrechten abgelegt sind. Dies gilt insbesondere für vertrauliche oder geheime Daten.

Müssen geschäftliche Daten temporär auf lokalen Geräten gespeichert werden, so hat die Benutzerin oder der Benutzer für entsprechende Sicherheit der Daten z.B. durch Verschlüsselung oder Sicherungskopien zu sorgen. Mitarbeitende sind für die Datensicherung lokaler Daten selbst verantwortlich. Die zentrale IT berät die Mitarbeitenden der HSG in Fragen der Sicherung lokaler Daten.

---

[5] Nachgetragen durch Beschluss des Senatsausschusses vom 15. Mai 2018; Inkraftsetzung per 15. Mai 2018.

[6] Zu diesen Systemen zählen beispielsweise auch vom Provider der Schweizer Universitäten, SWITCH, zur Verfügung gestellten Online-Speicherangebote in der Schweiz. Nähere Informationen befinden sich in der Weisung zur Datenhandhabung an der HSG.

Beispiele für geheime Daten (nicht abschliessend):

a. Besonders geschützte Personendaten (religiöse, weltanschauliche sowie politische Ansichten und Tätigkeiten; Gesundheit, Intimsphäre und Rassenzugehörigkeit; Verfahren und Massnahmen der Sozialhilfe; strafrechtliche sowie disziplinarische Verfahren und Sanktionen);
b. Persönlichkeitsprofile (Zusammenstellung von Daten, die eine Beurteilung der Persönlichkeit einer natürlichen Person erlaubt);
c. Daten, die bei Missbrauch eine Person erheblich benachteiligen;
d. Daten, die aufgrund vertraglicher Vereinbarungen oder gesetzlicher Vorschriften geheim zu halten sind.

Beispiele für vertrauliche Daten (nicht abschliessend):

a. Personendaten (Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, beispielsweise Kreditkartennummern oder Geburtsdaten);
b. Daten, die bei Missbrauch eine Person benachteiligen;
c. Daten mit finanzieller Relevanz;
d. Daten mit Archivierungspflicht.

Sollten geschäftliche Daten nicht mehr benötigt werden, so sind diese vor der Löschung dem Universitätsarchiv anzubieten, welches die Archivwürdigkeit beurteilt und für die Langzeitarchivierung der Daten Sorge trägt.

3.9 Sicherheit

Für HSG Geräte wird ein aktueller Virenschutz zentral von der zentralen IT zur Verfügung gestellt und gewartet. Der Virenschutz für private Geräte obliegt den Benutzerinnen und Benutzern, siehe dazu auch Ziff. 2.2.

Sicherungen von sowohl auf HSG-Geräten wie auch auf persönlichen Geräten abgelegten geschäftlichen Daten sind Sache der Benutzerinnen und Benutzer. Wenn HSG-Daten auf privaten Geräten gespeichert werden, so ist dieses zwingend mit einem PIN oder Passwortschutz zu versehen. Die zentrale IT stellt hierzu zentral verwalteten Speicher in Form von Netzlaufwerken und Kollaborationsplattformen zur Verfügung. Dort abgelegte Daten werden regelmässig gesichert und können bei Bedarf wiederhergestellt werden.

Benutzernamen und Passwörter (nachfolgend: Zugangsdaten) müssen regelmässig gewechselt und dürfen nicht an Dritte weitergegeben werden. Die Benutzerinnen und Benutzer haben geeignete Massnahmen zu treffen, damit ihre Zugangsdaten nicht durch andere Personen oder Systeme genutzt werden können. Beim Verlassen des IT-Arbeitsplatzes ist der Desktop oder Notebook zu sperren. Die am nicht-öffentlichen Netzwerk angeschlossenen Rechner müssen über einen aktivierten passwortgeschützten Bildschirmschoner verfügen. Büroräumlichkeiten mit Informatikmitteln müssen bei längeren Abwesenheiten und abends abgeschlossen werden.

Die Benutzerinnen und Benutzer verpflichten sich, bei der Arbeit mit Informatikmitteln die nötige Sorgfalt walten zu lassen und keine Aktionen oder Manipulationen durchzuführen, die andere Benutzerinnen und Benutzer stören oder den Betrieb oder die Sicherheit der IT-Systeme der HSG oder Externer beeinträchtigen könnten. Die Verwendung von Werkzeugen oder Methoden zum nichtautorisierten oder missbräuchlichen Eindringen in IT-Systeme ist untersagt.

3.10 Datenschutz Allgemein

Allgemeine Hinweise zum Datenschutz im HSG Webauftritt sind abrufbar unter http://www.unisg.ch/datenschutz. Die Details zum Datenschutz innerhalb des HSGnets im technischen Umgang mit Daten, den sog. Logfiles, finden sich in Anhang B dieses Dokuments.

3.11 Datenschutzklausel im AAI-Kontext

Der Dienst SWITCH-AAI[7] ermöglicht den teilnehmenden Institutionen den gegenseitigen Zugriff auf digitale Ressourcen. Zur Nutzung dieser Ressourcen ist die Bearbeitung ausgewählter Personendaten erforderlich, beispielsweise Name, Mailadresse, Herkunftsinstitution und organisatorische Zugehörigkeit.

Die Benutzerinnen und Benutzer der IT-Systeme der HSG erklären sich mit der im AAI-Kontext erforderlichen Datenbearbeitung einverstanden. Dieses Einverständnis umfasst insbesondere auch die Verwendung von Cookies[8] und den elektronischen Austausch, das Zwischenspeichern und das Speichern von personenbezogenen Autorisierungsattributen. Die Einwilligung der Benutzerinnen und Benutzer in den elektronischen Austausch dieser Autorisierungsattribute wird mit technischen Mitteln umgesetzt.

4 Nutzungszweck

Die IT-Infrastruktur der HSG wird grundsätzlich für Studienzwecke, Lehre, Forschung, Weiterbildung sowie Verwaltung zur Verfügung gestellt. Die kommerzielle Nutzung ausserhalb der HSG-Anstellung ist untersagt. Die private Nutzung ist zulässig, muss aber auf ein Minimum beschränkt werden.

Die missbräuchliche Nutzung von Informatikmitteln wird nicht akzeptiert. Als missbräuchlich gilt generell jede Verwendung der IT-Systeme der HSG, die

- im Widerspruch zum anwendbaren Recht steht,
- gegen diese Benutzungsrichtlinien verstösst oder
- Rechte Dritter verletzt.

Konkrete missbräuchliche Handlungen im IT-Kontext sind insbesondere:

a. Nutzung pornographischer, gewaltverherrlichender oder rassistischer Angebote gemäss Strafgesetzbuch (SR 311.0)
   (Ausnahme: Forschungsprojekte nach vorgängiger Zustimmung der vorgesetzten Stelle resp. des Abteilungsvorstands. Bei Studierenden ist der oder die verantwortliche Dozierende die zuständige Anlaufstelle.);
b. Zugriff auf Mails oder Rechner von Drittpersonen ohne deren Zustimmung;
c. Knacken von Passwörtern und sonstigen Zugangsberechtigungen;
d. Urheberrechts- und Datenschutzverletzungen.

Die Nutzungsberechtigung an Informatikmitteln erlischt direkt mit Beendigung des Anstellungsverhältnisses bzw. des Studiums.

---

[7] siehe https://www.switch.ch/aai/

[8] siehe https://de.wikipedia.org/wiki/Cookie

5 Überwachung des HSGnet und Ausschluss von der Benutzung

5.1 Überwachung des HSGnet

Die zentrale IT überwacht im Rahmen des geltenden Rechts (insbesondere im Rahmen des Daten- und Persönlichkeitsschutzes) die Einhaltung dieser Vorschriften. Bei Verdacht auf Zuwiderhandlung gegen die Vorschriften trifft die Leitung der zentralen IT in Abstimmung mit dem Generalsekretariat unter Beachtung der gesetzlichen Vorschriften geeignete Massnahmen, um weitere Verstösse zu verhindern, Beweise zu sichern, den ursprünglichen Zustand der Systeme wiederherzustellen und die Sicherheit und Funktionstüchtigkeit der Systeme zu gewährleisten.

Der Zugriff auf geschäftliche Mails anderer Personen ist gemäss Anhang A in bestimmten Fällen zulässig. Die zentrale IT hat bei der Auswertung von Logfiles Anhang B zu beachten.

5.2 Ausschluss von der Benutzung

Benutzerinnen und Benutzer, die den Vorschriften zuwiderhandeln oder das System auf eine andere Weise missbräuchlich verwenden, können von der Benützung des HSGnet ausgeschlossen werden. Besteht ein gravierender Verdacht auf missbräuchliche Verwendung, so ist die Leitung der zentralen IT in Abstimmung mit dem Generalsekretariat berechtigt, die persönliche Zugangsberechtigung zum HSGnet ohne Vorwarnung vorsorglich temporär zu sperren. Die Einleitung disziplinarischer sowie zivil- und/oder strafrechtlicher Schritte durch die Universitätsleitung bleibt vorbehalten.

5.3 Ausschlussverfahren

Vorsorglich ausgeschlossene Benutzerinnen und Benutzer, deren Benutzerkonto gesperrt wurde, müssen sich bei der zentralen IT melden. Nach Klärung der Sachlage kann die Leitung der zentralen IT das Benutzerkonto entweder wieder formlos öffnen lassen oder dem Verwaltungsdirektor Antrag über das weitere Vorgehen stellen. Der Rektor kann die definitive Sperrung des Benutzerkontos verfügen.

Die Verfügung kann beim Senatsausschuss angefochten werden (Art. 41 des Universitätsgesetzes, sGS 217.11).

Im Übrigen richten sich Verwaltungsverfahren und Rechtspflege nach dem Universitätsgesetz (sGS 217.11) und dem Gesetz über die Verwaltungsrechtspflege (sGS 951.1).

Bis zum Abschluss des Ausschlussverfahrens sind die für die Fortsetzung des Studiums notwendige Kommunikation und Information gewährleistet.

6 Schlussbestimmungen

Die HSG-IT-Benützungsvorschriften werden am 1. März 2016 erlassen und treten ab diesem Datum in Kraft. Sie ersetzen die HSGnet-Benützungsvorschriften vom 1. März 2016.

Im Namen des Senatsausschusses:

Der Rektor:	Die Generalsekretärin:
Prof. Dr. Thomas Bieger	lic.iur. Hildegard Kölliker

Anhang A. Zugriff auf Mails durch Dritte

1 Grundsatz

Weil die private Nutzung von Mail und Internet an der HSG nicht untersagt ist, muss grundsätzlich vom Vorhandensein privater Mails ausgegangen werden.

2 Private Mails

Private Mails dürfen auch im Rahmen der Stellvertretung durch Dritte nicht eingesehen werden, es sei denn, es liege eine Genehmigung der Besitzerin oder des Besitzers der Mailbox oder eine Anordnung der Strafverfolgungsbehörden vor.

3 Geschäftliche Mails

Die Einsicht in Mails mit eindeutig geschäftlichem Inhalt ist im Abwesenheitsfall im Rahmen der Stellvertretung zulässig.

Anhang B. Auswertungen von Logfiles

1 Entstehen von Logfiles

Die HSG setzt verschiedene technische Schutzmassnahmen gegen Missbrauch und technischen Schaden ihrer Informatiksysteme ein, beispielsweise Virenscanner, Firewall- und Netzwerkmonitoring. In diesem Rahmen werden von den Systemen sog. Logfiles (Protokollierungen) über die wichtigsten durchgeführten Aktivitäten geführt.

2 Anonyme Auswertung

Die anonyme Auswertung der Logfiles durch die zentrale IT ist jederzeit ohne vorherige Ankündigung zulässig. Sie bezweckt die statistische Auswertung nach systemspezifischen Kriterien. (Beispiele: beanspruchte Bandbreite, grösste Downloads, Anzahl versandter Mails.)

3 Pseudonyme Auswertung

Pseudonyme Auswertungen der Logfiles können auf Anordnung der Universitätsleitung stichprobenartig, aber nicht permanent, durchgeführt werden. Die HSG-Angehörigen sind über den Zeitraum der pseudonymen Auswertungen vorher in geeigneter Form zu orientieren. Pseudonyme Auswertungen bezwecken eine Auswertung der Logfiles nach pseudonymisierten, bestimmbaren Personen (Beispiel: Anzahl versandter Mails eines Instituts oder eines Verwaltungsbereichs während der Auswertungsperiode). Die Identität der von der pseudonymen Auswertung betroffenen Personen darf nicht leicht zu rekonstruieren sein.

4 Personenbezogene Auswertung

Falls im Rahmen anonymer und/oder pseudonymer Auswertungen Missbräuche festgestellt werden oder ein Missbrauchsverdacht entsteht, so können die Logfiles personenbezogen ausgewertet werden. Wenn sich der Missbrauchsverdacht nicht erhärtet, so wird die namentliche Auswertung der Logfiles umgehend eingestellt.
Im Falle einer festgestellten oder vermuteten Straftat werden die Logfiles separat gesichert. Die Universitätsleitung behält sich in solchen Fällen das Recht vor, Strafanzeige gegen die betreffende Person zu erstatten. Das Resultat allfälliger Ermittlungen wird durch die HSG vertraulich behandelt. Im Fall einer personenbezogenen Auswertung von Logfiles müssen die davon betroffenen Personen im Nachhinein informiert werden.