HCU Client-Sicherheit / HCU-Wissenschaftsnetz / HCU-Sondernetz / BYOD

Die IT-Sicherheits-Struktur der HCU wird von der HCU-Informationstechnik (HCU-IT) verwaltet.
Die Rechte und Pflichten sind in der HCU-Benutzungsordnung und in ergänzenden Einzelregelungen der HCU definiert.
Weitere Vorgaben, die den Betrieb von Verwaltungs- und Wissenschaftsnetz regeln, ergeben sich aus dem Netzkopplungsvertrag, der zwischen der HCU, der Finanzbehörde und Dataport, als zentralen Dienstleister der Freien und Hansestadt Hamburg, geschlossen wurde.
Diese Regelungen bilden zudem die Grundlage für die Basiszertifizierung der HCU gem. den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Ein wichtiger Aspekt ist die Sicherheit der an der HCU verwendeten Clients.
Hier unterscheidet die IT drei Kategorien von Clients mit unterschiedlichen Rechten und Pflichten:

IT-Services	**Wissenschaftsnetz MANAGED Clients** (normale Nutzer-Rechte)	**Sondernetz SELFMANAGED Clients** (mit lokalen Admin-Rechten)	**Privatgeräte** bzw. **BYOD** (maximale Rechte/Pflichten)
Client / Rechner-Anmeldung mit HCU-Benutzerkennung (AD)	**ja**	nein	nein
Drucker-Nutzung mit HCU-Benutzerkennung (mit AD SSO*****)	**ja**	nein	nein
Softwareverteilung Software- / Lizenz- / Sicherheits-Management (MDM)	**ja**	**ja**	nein
Support (Hard- und Software)	**ja**	NUR Herstellung des HCU-Sondernetz-Auslieferungs-Zustandes	nein
aktiver BIOS- / Firmware-Password als Schutz vor Daten-Zugriff durch unberechtigte	**ja**	**ja**	nein
Schutz vor Schadsoftware und Netzwerkangriffen	**ja**	**ja**	nein
HCU Team- / Home-Verzeichnisse (mit AD **SSO***)	**ja**	nein	nein
HCU Team- / Home-Verzeichnisse (ohne SSO*)	**ja**	**ja**	**ja**
eduroam	**ja**	**ja**	**ja**
VPN	**ja**	**ja**	**ja**

Active-**D**irectory (AD), **S**ingle-**S**ign-**O**n (**SSO**), Mobile-Device-Management (**MDM**), Bring-Your-Own-Device (**BYOD**)

Bring Your Own Device (BYOD) Clients**:**
Unter Bring-Your-Own-Device (BYOD) Clients/Geräte sind Rechner zusammengefasst, die von Privatpersonen und Mitgliedern / Studenten der HCU erworben und genutzt bzw. administriert werden. Über diese Geräte kann lediglich per VPN auf Team- und Homeverzeichnisse zugegriffen und eduroam genutzt werden.

- Geräte (Clients, Rechner, Computer und sonstige Devices) welche NICHT von der HCU beschafft wurden können nicht verwaltet werden.
- Geräte welche von der HCU beschafft wurden jedoch NICHT von der HCU Informationstechnik nach genannten Kriterien für SELFMANAGED und MANAGED Client verwaltet werden sind aus Sicherheitsgründen der Kategorie Bring-Your-Own-Device (BYOD) zugeordnet.

Für die Client/Geräte-Kategorie **"BYOD** Clients" wird kein Support geleistet.

SELFMANAGED und **MANAGED** Clients**:**

Alle HCU-IT verwalteten Clients/Geräte werden im HCU-Wissenschaftsnetz (MANAGED Clients mit normalen Nutzer-Rechten) oder HCU-Sondernetz (SELFMANAGED Clients mit lokalen Administratoren-Rechten) betrieben.

HCU Clients werden zentral von der HCU-IT beschafft und je nach Anforderung mit lizenzierter Software bestückt. Unter Windows und macOS werden Software, Lizenzen und Sicherheits-Einstellungen generell über eine Softwareverteilung gewährleistet. Software, Lizenzen und sogenannte Campus-Verträge und Lizenzen werden von der HCU-IT zentral verwaltet und auf aktuellem bzw. funktionsfähigem Stand gehalten.

Um die Funktionsfähigkeit der Lizenzen zu gewährleisten müssen diese über Softwareverteilung auf gültige bzw. wechselnde Lizenzschlüssel, Daten und / oder Server angepasst werden. Dies ist nur bei von der HCU-IT verwalteten Rechnern im HCU-Wissenschaftsnetz und HCU-Sondernetz möglich.

Clients im HCU-Wissenschaftsnetz und HCU-Sondernetz erhalten automatisch Sicherheits- und Virenschutz-Updates und werden bei erkannten Vorfällen von der IT eingefordert, um einen sicheren Betrieb der Hochschule sicherzustellen.
Alle HCU-IT verwalteten Geräte (macOS und Windows) werden vor Auslieferung auf einen funktionierenden BIOS- / EFI- bzw. Firmware- und Viren-Schutz inkl. Endpoint Protection geprüft. Dieser Schutz verhindert den Zugriff auf Client und Hochschuldaten durch unberechtigte / Dritte.
Unter macOS ist das Rechner/Client-Management durch ein sogenanntes Apple Mobile Device Management (MDM) umgesetzt, da dies von Seiten des Herstellers Apple zwingend vorausgesetzt wird. Apple-Hardware ist mit einem Hard- und Softwareschutz ausgestattet, der nur über ein MDM-System gewährleistet werden kann. Durch das MDM-Management der HCU werden Sicherheits-Einstellungen nach den Vorgaben der HCU umgesetzt und Software / Lizenzen aus dem Apple App-Store zur Verfügung gestellt. Apple Hardware wird automatisch an den Apple MDM-Service der HCU-Hamburg übertragen.

- **SELFMANAGED Clients (HCU-Sondernetz):**
  Die Nutzer-Anmeldung im HCU-Sondernetz (selbstadministrierte Geräte mit lokalen Admin-Rechten) erfolgt grundsätzlich mit lokalen Nutzern, die von den Mitarbeitern erstellt und verantwortet werden. Rechner im HCU Sondernetz erhalten einen lokalen Administrator und erhalten daher keine AD-Authentifizierung, da dies aus Sicherheits- und Datenschutz-Gründen nicht möglich ist.
  Für die Client/Geräte-Kategorie **“SELFMANAGED** Clients“ wird im Bedarfsfall nur Support für die Wiederherstellung der Arbeitsgeräte auf Basis des HCU-Sondernetz-Auslieferungs-Zustandes geleistet (nur Hard- und Software).

- **MANAGED Clients (HCU-Wissenschaftsnetz):**
  Clients im HCU-Wissenschaftsnetz (Nutzer haben keine lokalen Admin-Rechte) werden an den Active-Directory-Server (AD) der HCU gebunden. Die AD-Authentifizierung ermöglicht die Nutzer-Anmeldung mit einer HCU-Benutzerkennung und ermöglicht die „automatische“ Verbindung der HCU Team- / Home-Laufwerke und Drucken über Single-Sign-On (SSO).
  Für die Clients/Geräte-Kategorie “**MANAGED** Clients“ wird im Bedarfsfall Support für die volle Wiederherstellung der Arbeitsfähigkeit geleistet.