UNIVERSITÄT LEIPZIG

Informationen zu den Hochschulwahlen an der Universität Leipzig vom 21. Juni, 12:00 Uhr bis 28. Juni 2022, 12:00 Uhr

Stand der Informationen: 14.06.2022

1 Allgemeines

An der Universität Leipzig finden vom 21. Juni 2022, 12:00 Uhr bis 28. Juni 2022, 12:00 Uhr, Wahlen zum Senat, zum Erweiterten Senat, zu Fakultätsräten, Wahlen von Gleichstellungsbeauftragten und Stellvertretungen sowie die Wahl zum PromovierendenRat statt. Einzelheiten entnehmen Sie bitte den Wahlausschreibungen[1].

Die Wahlen werden als internetbasierte Online-Wahlen durchgeführt. Die Teilnahme an den Online-Wahlen erfolgt über einen aktuellen Webbrowser und kann prinzipiell von jedem internetfähigen Endgerät aus erfolgen. Eine spezielle Software ist nicht notwendig.

Als technische Plattform wird das Wahlsystem Polyas der POLYAS GmbH eingesetzt. Es ist einfach und intuitiv zu bedienen.

Die Wahlen zum Senat, zum Erweiterten Senat, zu Fakultätsräten sowie die Wahlen von Gleichstellungsbeauftragten und ggf. ihrer Stellvertretungen[2] werden in *einem Verfahren* zusammengefasst. Die Wahlen zum PromovierendenRat[3] stellen ein separates Wahlverfahren dar.

2 Autorisierung für die Teilnahme an den Online-Hochschulwahlen

Die Wahlberechtigten erhalten einen Benutzernamen (Wähler-ID), ein Passwort und einen Internetlink für die Wahl per E-Mail zugeschickt. Damit ist eine direkte Authentifizierung im Wahlsystem von Polyas möglich. Nach Eingabe der Wähler-ID und des Passworts im Wahlsystem Polyas kann die Stimmabgabe durchgeführt werden.

Der Benutzername (Wähler-ID) und das Passwort werden an die dem Wahlamt bekannte E-Mailadresse geschickt. Die Zusendung erfolgt aus Sicherheitsgründen in zwei unabhängigen E-Mails.

Sollten Sie keine Wähler-ID und kein Passwort zugeschickt bekommen haben, wenden Sie sich bitte an das Wahlamt der Universität Leipzig (siehe Kontakt am Ende des Dokumentes).

---

[1] https://www.uni-leipzig.de/universitaet/service/ordnungen-und-wahlen/wahlen/

[2] https://intranet.uni-leipzig.de/fileadmin/user_upload/intranet/Dezernat_2/Akademische_Angelegenheiten/20220413_Wahlausschreibung_Gremien_GB_gez.pdf

[3] https://intranet.uni-leipzig.de/fileadmin/user_upload/intranet/Dezernat_2/Akademische_Angelegenheiten/20220413_Wahlausschreibung_ProRat_gez.pdf

3 Sicherheitshinweise

3.1 Allgemeine Sicherheitshinweise

Die Teilnahme der Wahlberechtigten an den Online-Hochschulwahlen soll auf einem individuell genutzten Computer mit Internetanschluss erfolgen, über den die abgegebenen Stimmen verschlüsselt an das Wahlsystem von Polyas übertragen werden. Die Beachtung der hier empfohlenen Sicherheitsmaßnahmen soll sicherstellen, dass geeignete Vorkehrungen getroffen wurden, um ein Mindestmaß an Sicherheit zu gewährleisten, insbesondere um Angriffe durch Schadprogramme und ähnliche dienstbehindernde Attacken auf den Computer oder das Wahlsystem zu vermeiden und die Einhaltung des Wahlgeheimnisses zu gewährleisten.

3.2 Nutzbarkeit des Wahlsystems trotz technischer oder persönlicher Einschränkungen

Das Wahlsystem von Polyas ist grundsätzlich für alle Wahlberechtigten barrierearm zugänglich. Unabhängig von körperlichen oder technischen Möglichkeiten ist die Teilnahme an den Online-Hochschulwahlen weitgehend uneingeschränkt ohne fremde Hilfe durchführbar. Dies schließt sowohl die Nutzung durch Personen mit und ohne gesundheitliche Beeinträchtigungen als auch die Nutzung mit technischen Einschränkungen (z.B. Textbrowser oder PDA) grundsätzlich ein. Das Vorlesen der dargestellten Informationsangebote über spezielle Computerprogramme (screen reader) oder die Ausgabe in Braille-Schrift für Blinde und sehbehinderte Personen ist mit entsprechenden Hilfsmitteln möglich.

3.3 Wahlsystem

Für die Online-Hochschulwahlen kommt das Wahlsystem Polyas der POLYAS GmbH[4] zum Einsatz. Dieses besteht aus drei technischen Modulen. Das Modul „Wählerverzeichnis“ enthält ein anonymes Verzeichnis, in dem lediglich sog. Wähler-IDs und keine personenbezogenen Daten enthalten sind. Das davon getrennte Modul „Wahlfreigabe“ (Validator) erteilt die Wahlmöglichkeit und das gleichfalls unabhängige Modul „Wahlurne“ wird für die Aufbewahrung und Zählung der Stimmen eingesetzt. Als Übertragungskanal wird das Internet genutzt. Die Kommunikation zwischen den Modulen erfolgt ausschließlich verschlüsselt über HTTPS[5].

Daten, die auf die persönliche Identität von Wahlberechtigten schließen lassen könnten, werden ausdrücklich nicht an Polyas übermittelt bzw. im Wahlsystem gespeichert.

Die Sicherheit der für den Betrieb eingesetzten Server, die streng getrennt arbeiten, sowie die dort eingesetzten Verfahren werden durch die Firma POLYAS GmbH nach allgemein anerkannten Sicherheitsstandards, wie z.B. ISO 27017 oder ISO 27001, gewährleistet.

[4] www.polyas.de

[5] HTTPS ist ein Protokoll zum verschlüsselten Surfen auf Internetseiten und wird durch alle gängigen Internetbrowser unterstützt.

3.4 Sicherheitstechnische Anforderungen an den Computer, der zur Teilnahme an den Online-Hochschulwahlen genutzt wird

Zur Teilnahme (Durchführung des Wahlvorgangs) ist ein handelsüblicher Computer mit funktionierendem Internetanschluss erforderlich, wie er in den Einrichtungen der Universität Leipzig und auch in vielen Privathaushalten üblich ist. Es wird empfohlen, ausschließlich Computerarbeitsplätze in vertrauenswürdigen Umgebungen zu nutzen, bei denen die grundsätzliche Einhaltung der in diesem Dokument empfohlenen Sicherheitsmaßnahmen sichergestellt wird. Von der Nutzung von Computerarbeitsplätzen in nicht vertrauenswürdigen Umgebungen wird aus Sicherheitsgründen abgeraten. Wahlberechtigte sind grundsätzlich selbst dafür verantwortlich, dass die Beachtung der hier empfohlenen Sicherheitsmaßnahmen am genutzten Computer gegeben ist.

Die Stimmabgabe über ein Smartphone ist möglich. Es gelten dieselben Sicherheitsanforderungen wie für Computer.

Soweit Wahlberechtigte keinen dienstlichen oder privaten Zugang zu einem für die Stimmabgabe geeigneten Gerät haben, steht zur Teilnahme an den Online-Hochschulwahlen ein Computer der Universität zur Verfügung. Der Raum ist barrierefrei zugänglich. Es ist eine Voranmeldung per Telefon oder E-Mail im Wahlamt erforderlich.

3.5 Geheimhaltung der Zugangsdaten

Bitte achten Sie immer darauf, dass Unbefugten weder Ihr Uni-Login und Ihr Passwort noch der Ihnen zugesandte Benutzername (Wähler-ID) und das zugehörige Passwort bekannt werden. Halten Sie diese Informationen stets unter Verschluss und geben Sie diese nicht an Dritte weiter.

3.6 Nutzung des Computers ohne administrative Rechte

Es wird empfohlen, das Internet nur mit einem Benutzungskonto ohne Administrationsrechte zu nutzen, um zu verhindern, dass sich Schadprogramme unbeabsichtigt installieren können. Schadprogramme sind zur dauerhaften Installation auf Computern meist darauf angewiesen, dass angemeldete Benutzerinnen und Benutzer über Administrationsrechte verfügen. Hinweise zur Einrichtung eines Benutzungskontos ohne diese Rechte finden sich in der Dokumentation des Betriebssystems.

3.7 Einsatz von Computerprogrammen aus vertrauenswürdigen Quellen

Das Installieren und Starten von Programmen, die von Unbekannten oder ungefragt von Bekannten per E-Mail oder aus anderen unsicheren Quellen übermittelt wurden, sollte unterbleiben. Vorsicht: Auch Bildschirmschoner sind Programme. Sofern auch nur geringe Zweifel an der Vertrauenswürdigkeit von Programmen bestehen, sollte auf eine Installation auf dem Computer verzichtet werden.

3.8 Internetbrowser

Es ist darauf zu achten, dass die eingesetzte Internetbrowser-Software[6] aus vertrauenswürdigen Quellen bezogen wurde, so dass sichergestellt ist, dass es sich um unveränderte Originalsoftware handelt. Folgende Internetbrowser werden empfohlen: Chrome, Firefox, Internet Explorer (ab Version 11), Opera,

[6] Ein Internet-Browser ist eine Anzeigesoftware für Internetseiten. Bekannte Browser sind Firefox, Opera oder Chrome.

Safari, Edge. Wichtig ist, dass der Internetbrowser regelmäßig aktualisiert wird, um die Sicherheit der Internetverbindung zu wahren. Beim Bekanntwerden von Sicherheitsproblemen veröffentlichen die Softwarehersteller in der Regel zeitnah fehlerbereinigte Versionen (Updates). Deshalb sind regelmäßig neue Sicherheitsupdates für das Betriebssystem und den Internetbrowser auf dem Computer einzuspielen, z.B. für Microsoft-Produkte mit Hilfe der Windows-Update-Funktion.

3.9 Unterstützung von sog. Cookies

Nach der Anmeldung am Wahlsystem möchte der POLYAS-Server einen sog. Cookie auf dem Computer speichern. Dieser „Session Cookie“ enthält **keine personenbezogenen Daten** und wird auch nicht von POLYAS ausgewertet, sondern dient allein zur Stimmabgabe. Sobald der Internetbrowser nach der Stimmabgabe geschlossen wird, **wird auch der Cookie automatisch gelöscht. Daher sollte dieser Cookie erlaubt werden**, um von einer höheren Sicherheit während der Stimmabgabe zu profitieren.

3.10 Einstellungen der Internetbrowser

Die Internetbrowser verschiedener Herstellerfirmen unterscheiden sich zwar in ihrer Handhabung und Konfiguration, einige Hinweise haben aber allgemeingültigen Charakter. Folgende Punkte sollten beachtet werden:

- Während der Teilnahme an den Online-Hochschulwahlen ist darauf zu verzichten, in einem zweiten Browser-Fenster oder -Tab andere Internetseiten mit nicht vertrauenswürdigen Inhalten anzuzeigen.
- Die Internetseiten von Polyas benötigen für ihre Funktionsfähigkeit kein Microsoft ActiveX für die Anzeige aktiver Inhalte. Da mit Hilfe von ActiveX auch Zugriffe auf die Daten und Komponenten Ihres Computers möglich sind, wird empfohlen, ActiveX im Internetbrowser generell zu deaktivieren (nur Internet Explorer und Edge).
- Die Aktivierung von JavaScript, die häufig zur Unterstützung von benutzungsbezogenen Funktionen in internetbasierten Anwendungen eingesetzt wird, ist erforderlich.
- Der Internetbrowser sollte so eingestellt sein, dass verschlüsselte Seiten und so genannte Cookies zum Speichern Ihrer persönlichen Einstellungen auf Webseiten angenommen werden. Nach Beendigung des Wahlvorgangs können mit dem Schließen des Internetbrowsers alle Cookies gelöscht werden.
- Die Funktion, welche Benutzernamen und Kennwörter für die automatische Eingabe bei späteren Aufrufen speichert, sollte nicht genutzt werden. Dazu ist bei einer entsprechenden Abfrage durch Ihren Internetbrowser „Anmeldedaten speichern?“ (o.ä.) „Nein“ bzw. „Nicht speichern“ auswählen.
- Der sogenannte Cache (Speicherbereich, in dem zuvor angezeigte Seiten gespeichert werden) des Internetbrowsers sollte automatisch nach jeder Sitzung gelöscht werden (siehe entsprechende Voreinstellungen des Internetbrowsers). Durch diese Maßnahme wird verhindert, dass die auf dem Computer aufgerufenen Seiten nachträglich eingesehen werden können. Aktuelle Internetbrowser unterstützen das Surfen im sog. „Privaten Modus“. Dabei werden keine Daten über Webseitenbesuche auf dem Computer gespeichert. Hinweise zur Aktivierung des „Privaten Modus“ finden sich auf den Hilfeseiten der Internetbrowseranbieter.

3.11 Sichere verschlüsselte Übertragung

Grundlage einer sicheren Internetverbindung ist die Verwendung eines sicheren Protokolls für die verschlüsselte Übertragung der Daten per SSL (SSL – Secure Sockets Layer bezeichnet ein Netzwerkprotokoll zur sicheren Übertragung von Daten u.a. von Internetseiten). Das Bestehen einer solchen sicheren

SSL-Verbindung wird Ihnen bei Verwendung von Firefox, Chrome, Edge und Internet Explorer durch ein **„geschlossenes Schloss-Symbol“** angezeigt. Bitte achten Sie darauf, dass nach der Anmeldung am Wahlsystem von Polyas während der gesamten Verbindungsdauer dieses Symbol dargestellt wird. Durch Doppelklick auf das jeweilige Symbol werden weitere Informationen zum Sicherheitszertifikat angezeigt. Die Darstellung ist abhängig vom verwendeten Internetbrowser. Das Serverzertifikat des Wahlsystems von Polyas kann anhand der dazu gehörenden sogenannten elektronischen Fingerabdrücke (fingerprints) geprüft werden. Hierzu ist zunächst die Internet-Adresse (URL) zu überprüfen, die aufgerufen wurde. **Die Internetadresse muss während einer Sitzung mit „https://“ angezeigt werden und nicht mit „http://“. Das 's' in https signalisiert eine sichere Verbindung.**

Das Server-Zertifikat des Wahlsystems von Polyas (https://election.polyas.com/) hat folgende Fingerprints:

- SHA-1 Fingerprint:

  3D:E5:EA:28:A8:DB:54:82:04:9E:3F:A6:75:0F:FD:8C:94:BA:BA:F8

- SHA-256 Fingerprint:

  FD:73:DE:02:78:28:23:66:C4:90:5A:DF:99:D0:B4:CE:A3:FE:77:DF:7A:CD:F0:48:2B:14:4A:3C:52:6D:78:CD

Nur wenn diese Daten angezeigt werden, besteht eine sichere und verschlüsselte Verbindung. Sollten andere Daten angezeigt werden, ist die Verbindung sofort zu beenden und umgehend der Servicedesk des Universitätsrechenzentrums zu informieren (Kontaktdaten siehe unten).

3.12 Automatische Zeitüberwachung/Abmelden vom Wahlsystem

Ein Verlassen des Wahlvorgangs ist ordnungsgemäß über die Schaltfläche „Stimmabgabe abbrechen“ jederzeit möglich. Der Wahlvorgang wird automatisch abgebrochen, wenn ca. 15 Minuten lang keine Eingabe erfolgt ist. Die bis dahin erfolgten Eingaben werden nicht gespeichert. In beiden vorgenannten Fällen muss eine erneute Anmeldung am Wahlsystem erfolgen. Die Eingaben sind erneut zu tätigen.

3.13 Schutz vor Schadsoftware / Computerviren

Computerviren sind Schadprogramme, die nicht kontrollierbare Veränderungen am Status der Hardware (z.B. Netzwerkverbindungen), am Betriebssystem oder an der Software vornehmen (Schadfunktion). Computerviren können die Informationssicherheit erheblich beeinträchtigen. Deshalb ist ein Virenscanner auf dem Computer zu installieren und damit sind regelmäßig alle Dateien auf Viren zu überprüfen (scannen). Der Virenscanner ist durch das regelmäßige Einspielen von Updates aktuell zu halten. Das Universitätsrechenzentrum bietet allen Mitgliedern der Universität eine Antivirensoftware zum Download an[7].

3.14 Schutz vor dem Ausspähen von Benutzerdaten

Durch sogenannte „Trojanische Pferde“ (als „Trojanisches Pferd“, auch kurz „Trojaner“ genannt, bezeichnet man ein Programm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen der nutzenden Person eine andere, meist unerwünschte Funktion erfüllt) können vertrauliche Daten ausgespäht und während einer Internetsitzung unbemerkt an Dritte übertragen werden. Dadurch besteht das

[7] https://www.urz.uni-leipzig.de/unsere-services/servicedetail/service/sicherheitssoftware-sophos-antivirus

potenzielle Risiko, dass Ihre Zugangsdaten bei der Eingabe über die Tastatur abgefangen und an Unberechtigte gesendet werden, die dann z.B. an Ihrer Stelle wählen könnten. Einen hundertprozentigen Schutz gegen Trojaner gibt es nicht. Software sollte nur aus vertrauenswürden Quellen installiert werden.

Angreifer können versuchen, mit sogenannten Phishing-Nachrichten direkt zur Preisgabe von Zugangsdaten auf gefälschten Webseiten zu verleiten. Hinweise zur Erkennung von gefährlichen E-Mails, gefälschten Nachrichten und Webseiten sind im Intranet der Universität[8] zu finden.

Weiterhin sollte Software zur Fernwartung (z.B. TeamViewer) deaktiviert sein, um sicherzustellen, dass keine unbefugte Person den Wahlvorgang mitverfolgen kann und damit das Wahlgeheimnis verletzt.

3.15 Überwachung des Datenverkehrs vom und zum Internet

Zusätzlichen Schutz vor „Trojanischen Pferden“ können auch sogenannte „Personal Firewalls“ bieten, die als lizenzierte, kostenpflichtige Produkte oder als Freeware zur Verfügung stehen. Dies sind Programme, die, richtig eingestellt, den gesamten Datenverkehr von und zum Internet überwachen. Sie können dadurch erkennen und verhindern, wenn ein anderes Programm als der von Ihnen benutzte Browser versucht, Datenpakete über das Internet zu versenden.

Bezugsquellen für Virenschutz-Software, Personal Firewalls und Anti-Spy-Programme finden sich in Computer-Zeitschriften sowie an vielen Stellen im Internet. Zur von der Universität verwendeten Software „Sophos Endpoint Security“ finden Beschäftigte Informationen auf dieser Webseite des Universitätsrechenzentrums[9].

Weitere nützliche Tipps zum Thema Sicherheit finden sich im Internet unter https://www.bsi-fuer-buerger.de und im Intranet der Universität Leipzig unter https://intranet.uni-leipzig.de/zentralverwaltung/referat-fuer-datenschutz-und-informationssicherheit/sicherheitshinweise/.

4 Hilfestellungen bei Problemen und Fragen

Alle Informationen zur Durchführung des Wahlvorgangs stehen auf den Webseiten der Universität Leipzig[10]. Im Wahlsystem von Polyas wird Schritt für Schritt durch die Stimmabgabe mit Hinweisen und Erläuterungen durchgeleitet.

Sofern sich in Bezug auf den dienstlichen Computer technische Probleme oder Fragen ergeben sollten, wenden Sie sich bitte unmittelbar an die zuständigen IT-Verantwortlichen in Ihrem Bereich (Fakultät, Institut, Arbeitsgruppe…) oder an den Servicedesk des Universitätsrechenzentrums.

Bei allgemeinen Fragen oder Unklarheiten zur Wahl wenden Sie sich bitte an das Wahlamt der Universität Leipzig. Dies gilt auch, wenn eine sicherheitsrelevante Unregelmäßigkeit bemerkt wird oder ein Verdacht auf Manipulation besteht. In diesem Fall bitten wir um unverzügliche Information.

[8] https://intranet.uni-leipzig.de/zentralverwaltung/referat-fuer-datenschutz-und-informationssicherheit/sicherheitshinweise/e-mails/

[9] https://www.urz.uni-leipzig.de/unsere-services/servicedetail/service/sicherheitssoftware-sophos-antivirus

[10] https://www.uni-leipzig.de/universitaet/service/ordnungen-und-wahlen/wahlen/

Kontakt

Universitätsrechenzentrum

Servicedesk

Sprechzeit: Mo. bis Fr. zwischen 9 Uhr und 15 Uhr

Tel.: +49 341 97-33333

E-Mail: servicedesk@uni-leipzig.de

Kontaktformular: https://service.rz.uni-leipzig.de/servicedesk-kontaktformular/

Bitte vorrangig per E-Mail oder Kontaktformular an den Servicedesk wenden. Auf Grund hoher Anfragen kann es zu verzögerten Antwortzeiten kommen.

Kontakt

Wahlamt der Universität Leipzig

wahlamt@uni-leipzig.de

Tel.: +49 341 97-32008

https://www.uni-leipzig.de/universitaet/service/ordnungen-und-wahlen/wahlen/