# Hinweise zu den Online-Wahlen an der Martin-Luther-Universität Halle-Wittenberg 2022

## 1. Allgemeines

In diesem Jahr finden die Wahlen der Vertreter*innen der Mitgliedergruppen 1 (Hochschullehrer*innen), 2 (wissenschaftliche Mitarbeiter*innen), 3 (Studierende) und 4 (sonstige Mitarbeiter*innen) zum Senat und zu den Fakultätsräten, die Wahlen zum Studierendenrat und zu den Fachschaftsräten sowie die Wahlen zu den Gleichstellungskollegien und Promovierendenvertretungen statt. Wählen dürfen damit in diesem Jahr:

- alle Studierenden,
- alle Beschäftigten der Mitgliedergruppe 1, 2 und 4
- alle Promovierenden der Universität, die in der elektronischen Doktorandenverwaltung HalDoc registriert sind

Die Wahlen werden erstmals als internetbasierte Online-Wahlen durchgeführt. Die Online-Wahl erfolgt über einen Webbrowser (s. dazu unter 3.) und kann somit von jedem internetfähigen Endgerät aus erfolgen. Eine Spezialsoftware ist nicht notwendig.

Als technische Plattform wird das Wahlsystem Polyas der POLYAS GmbH mit einer auf die MLU-spezifischen Bedürfnisse angepassten Nutzerführung des Wahlsystems eingesetzt, die einfach und intuitiv zu bedienen ist.

Polyas wurde 2016 durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland erstmals das Zertifikat für eine Online-Wahl-Software verliehen und im Juni 2021 erneut durch das BSI zertifiziert. Es basiert auf den Common Criteria für Online-Wahlen und dem Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, die sich aus den allgemeinen Wahlgrundsätzen ableiten. Dementsprechend sind Online-Wahlen in der Konfiguration Polyas CORE 2.5.0 nach Maßgabe der BSI-Anforderungen sicher und erfüllen die Ansprüche an das demokratische Wahlrecht.

## 2. Sicherheitshinweise

**Allgemeine Sicherheitshinweise**

Die Abstimmung durch die Wahlberechtigten soll bei den als Online-Wahl durchgeführten Wahlen auf einem individuell genutzten Computerarbeitsplatz mit Internetanschluss erfolgen, über den die abgegebenen Stimmen verschlüsselt an das Wahlsystem übertragen werden. Die Beachtung der hier empfohlenen Sicherheitsmaßnahmen soll sicherstellen, dass geeignete Vorkehrungen getroffen sind, um ein Mindestmaß an Sicherheit zu gewährleisten: etwa, um Angriffe durch „Computerviren, Würmer, Trojaner“ (Schadprogramme) und ähnliche dienstbehindernde Attacken auf den Computerarbeitsplatz oder Wahlservern zu vermeiden oder um die Einhaltung des Wahlgeheimnisses zu gewährleisten.

**Nutzbarkeit des Wahlsystems trotz technischer oder persönlicher Einschränkungen**

Die Wahlanwendung ist grundsätzlich für alle berechtigten Nutzerinnen und Nutzer barrierearm zugänglich. Unabhängig von körperlichen oder technischen Möglichkeiten ist die Online-Wahl 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 (Screenreader) oder die Ausgabe in Braille-Schrift für Blinde und sehbehinderte Personen ist mit entsprechenden Hilfsmitteln möglich.

**Wahlsystem**

Bei der Online-Wahl kommt die Anwendung „Polyas“ der POLYAS GmbH (www.polyas.de) zum Einsatz. Diese besteht aus drei technischen Modulen. Das Modul „Wählerverzeichnis“ enthält ein anonymes Verzeichnis, in dem lediglich die Wahlnummern 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 bei der Online-Wahl das Internet genutzt. Die Kommunikation zwischen den Modulen erfolgt über das HTTPS-Protokoll ausschließlich verschlüsselt. Daten, die auf die persönliche Identität von Wahlberechtigten schließen lassen könnten, werden ausdrücklich nicht in Polyas gespeichert. Die Sicherheit der für den Betrieb eingesetzten Server, die streng getrennt arbeiten, sowie die dort eingesetzten Verfahren werden durch die technischen Betreiber nach allgemein anerkannten Sicherheitsstandards gewährleistet.

**Sicherheitstechnische Anforderungen an den Computerarbeitsplatz, der zur Durchführung der Wahl genutzt wird**

Zur Durchführung des Wahlvorgangs ist ein handelsüblicher Computerarbeitsplatz mit funktionierendem Internetanschluss erforderlich, wie er in den Einrichtungen der Martin-Luther-Universität und auch in vielen Privathaushalten üblich ist. Es wird empfohlen, ausschließlich Computerarbeitsplätze in vertrauenswürdigen Umgebungen zu nutzen, bei denen die grundsätzliche Einhaltung der empfohlenen Sicherheitsmaßnahmen im Allgemeinen 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 Computerarbeitsplatz gegeben ist.

Diese Sicherheit wird z.B. auch in den Computerpools der Universität gewährleistet, sofern kein geeigneter Arbeitsplatz zur Verfügung steht. Wenn diese pandemiebedingt nicht geöffnet sein sollten, besteht alternativ die Möglichkeit, für die Teilnahme an der Online-Wahl während des Wahlzeitraumes einen PC im Wahlamt zu nutzen. Zur Einhaltung der Hygieneregeln wird hierfür um telefonische Voranmeldung im Wahlamt gebeten.

**Benutzer-Autorisierung für die Teilnahme an der Online-Wahl**

**a) Studierende**

Die wahlberechtigten Studierenden nutzen für die Teilnahme an der Online-Wahl zunächst ihren Zugang zum Löwenportal für Studierende und melden sich dort mit ihrer persönlichen Benutzerkennung und zugehörigem Passwort an. Im Wahlzeitraum vom 09.-16.05.2022 finden die Studierenden im Löwenportal im Funktionsmenü den Unterpunkt „Online-Wahlen“. Der bzw. die Studierende findet an dieser Stelle einen individualisierten und temporär gültigen Link (SecureLink) zum Wahlsystem. Über diesen Link erfolgt eine Weiterleitung zum Wahlsystem. Dort ist keine erneute Authentifizierung mehr notwendig und alle Wahlberechtigten können direkt mit der Stimmabgabe beginnen. Die Identität der Wähler ist dabei zu jeder Zeit geschützt.

**b) Beschäftigte**

Aus technischen Gründen ist derzeit leider noch keine Authentifizierung mittels SecureLink für Beschäftigte möglich. Die bei den diesjährigen Hochschulwahlen wahlberechtigten Beschäftigten erhalten daher für die Authentifizierung im Wahlsystem von Polyas eine jeweils individuell erzeugte Wähler-ID und ein Passwort. Diese werden in zwei unabhängigen E-Mails an die dienstliche E-Mail-Adresse der Beschäftigten übersandt. Sofern einzelne Beschäftigte über keine dienstliche E-Mail-Adresse verfügen sollten, werden die Zugangsdaten vom Wahlamt an eine andere bekannte E-Mail-Adresse oder per Hauspost an die dienstliche Anschrift versendet. Nach Eingabe der jeweiligen Wähler-ID und des Passworts im Wahlsystem von Polyas kann die Stimmabgabe durchgeführt werden.

**Geheimhaltung der Zugangsdaten**

Bitte achten Sie unbedingt darauf, dass Sie Ihren Zugang zum Löwenportal (Studierende) bzw. die Ihnen zugesandten Zugangsdaten (Beschäftigte) stets unter Verschluss zu halten haben und unberechtigte Dritte keinen Zugriff auf diese Daten bekommen dürfen.

**Nutzung des Computerarbeitsplatzes ohne administrative Rechte**

Wir empfehlen Ihnen dringend, das Internet nur mit einem Benutzerkonto ohne Administrationsrechte zu nutzen und zu verhindern, dass sich Schadprogramme unbeabsichtigt installieren können. Schadprogramme sind zur dauerhaften Installation auf fremden Rechnern meist darauf angewiesen, dass angemeldete Benutzerinnen und Benutzer über Administrationsrechte verfügen. Wie Sie ein solches Benutzungskonto ohne diese Rechte einrichten, können Sie der Dokumentation Ihres Betriebssystems entnehmen.

**Internetbrowser**

Achten Sie bitte darauf, dass Sie die eingesetzte Browser-Software aus vertrauenswürdigen Quellen bezogen haben, so dass sichergestellt ist, dass es sich um unveränderte Originalsoftware handelt. Bitte setzen Sie nur die folgenden Browser ein: Chrome, Firefox, Internet Explorer (ab Version 11), Opera, Safari, Edge. Wichtig ist, dass Sie ihren Browser regelmäßig aktualisieren, um die Sicherheit Ihrer Internetverbindung zu wahren. Beim Bekanntwerden von Sicherheitsproblemen veröffentlichen die Softwarehersteller in der Regel zeitnah fehlerbereinigte Versionen (Updates). Informieren Sie sich daher regelmäßig über neue Sicherheitsupdates für das Betriebssystem und den Internet-Browser Ihres Computerarbeitsplatzes, z.B. für Microsoft-Produkte mit Hilfe der Windows-Update-Funktion, oder fragen Sie als Beschäftigte/r Ihre zuständige IT-Betreuung.

**Einstellungen der Browser**

Die Internet-Browser verschiedener Herstellerfirmen unterscheiden sich zwar in ihrer Handhabung und Konfiguration, einige Hinweise haben aber allgemeingültigen Charakter. Folgende Punkte sollten Sie beachten:

- Sie sollten während der Nutzung von Polyas darauf verzichten, in einem zweiten Browser-Fenster oder -Tabs andere Internetseiten mit nicht vertrauenswürdigen Inhalten anzuzeigen.
- Die Internetseiten von Polyas benötigen für ihre Funktionsfähigkeit nicht das von Microsoft entwickelte Softwarekomponenten-Modell 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 Browser generell zu deaktivieren (nur Internet Explorer).
- Die Aktivierung der objektbasierten Programmiersprache JavaScript, die häufig zur Unterstützung von benutzungsbezogenen Funktionen in internetbasierten Anwendungen eingesetzt wird, ist erforderlich.
- Stellen Sie Ihren Browser so ein, dass verschlüsselte Seiten und so genannte Cookies zum Speichern Ihrer persönlichen Einstellungen auf Webseiten gespeichert werden.
- Deaktivieren Sie die Funktion, welche Benutzernamen und Kennwörter für die automatische Eingabe bei späteren Aufrufen speichert, d.h. wählen Sie bei einer entsprechenden Abfrage durch Ihren Browser „Anmeldedaten speichern?“ (o.ä.) „Nein“ bzw. „Nicht speichern“ aus. Im Übrigen finden Sie diese Einstellungen beim Internet Explorer unter „Internetoptionen/Inhalte/AutoVervollständigen“, bei anderen Browsern heißen sie z.B. Kennwort- oder Password-Manager.
- Sorgen Sie dafür, dass der sogenannte Cache (Speicherbereich, in dem zuvor angezeigte Seiten gespeichert werden) des Browsers nach jeder Sitzung gelöscht wird. Durch diese Maßnahme können Sie verhindern, dass die auf dem von Ihnen benutzten Computerarbeitsplatz aufgerufenen Seiten nachträglich angesehen werden können. Sie können die Browser aber auch im „Privaten Modus“ verwenden. Dabei nutzen Sie das Internet, ohne dass der Browser irgendwelche Daten über Ihre Webseitenbesuche auf Ihrem Rechner speichert. Für den Firefox kann der „Private Modus“ unter Windows & Linux mit Shift + CTRL / Strg + P und Mac OSX mit Shift + ⌘ + P gestartet werden.

**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 und Internet Explorer durch ein „geschlossenes Schloss-Symbol“ angezeigt. Bitte achten Sie darauf, dass nach der Anmeldung am Wahlserver während der gesamten Verbindungsdauer dieses Symbol dargestellt wird. Durch Doppelklick auf das jeweilige Symbol werden Ihnen weitere Informationen zum Sicherheitszertifikat angezeigt. Die Darstellung ist abhängig von dem von Ihnen eingesetzten Internet-Browser. Die Serverzertifikate der Wahlserver können Sie anhand der dazu gehörenden sogenannten elektronischen Fingerabdrücke (fingerprints) prüfen. Hierzu überprüfen Sie bitte wie zuvor beschrieben die Internet-Adresse (URL), mit der Sie verbunden sind. Die Internetadresse muss während einer Sitzung mit „https://“ angezeigt werden und **nicht** mit „http://“. Das 's' in https signalisiert eine sichere Verbindung.

Das Zertifikat des Servers für das Löwenportal für Studierende (https://loewenportal.uni-halle.de/ ) hat folgende Fingerprints:

- SHA-1 Fingerprint:

  01:57:99:E2:B4:E6:7E:6F:A2:A6:36:A3:6C:3B:F8:34:8F:39:38:4A

- SHA-256 Fingerprint:

  ED:A7:1A:DF:21:F3:5D:39:2C:91:39:A4:6A:12:BE:5B:AA:15:0D:AA:58:F4:5E:03:9B:B2:8C:CA:A0:B2:34:2A

Das Zertifikat des Wahl-Servers (https://election.polyas.com/) hat folgende Fingerprints:

- SHA-1 Fingerprint :

  34 58 82 2D 3A 0D 1C 78 D2 14 78 56 1F 08 1E 2A 71 C4 27 0D

- SHA-256 Fingerprint:

  0D 15 9F 30 41 04 4C 9D AD 59 1D F4 1A 69 32 CD 5F 44 7D 9E 05 10 DD BB 98 F5 C5 A0 27 94 5F 3D

Nur wenn Sie diese Daten angezeigt bekommen, besteht eine sichere und verschlüsselte Verbindung zum Wahlserver. Sollten Sie andere Daten angezeigt bekommen, beenden Sie die Verbindung sofort und informieren Sie bitte umgehend das Wahlamt der Universität (Kontaktdaten siehe unten).

**Automatische Zeitüberwachung/Abmelden vom Wahlsystem**

Verlassen Sie die Wahl bitte ordnungsgemäß über die Schaltfläche „Stimmabgabe abbrechen“, wenn Sie den Wahlvorgang ab- oder unterbrechen wollen. Sollten Sie einmal versäumt haben, die Wahlanwendung zu beenden oder längere Zeit Ihren Rechner unbeaufsichtigt lassen, bricht die im System eingebaute Zeitsperre aus Sicherheitsgründen den Wahlvorgang ab, sobald ca. 15 Minuten lang keine Eingabe erfolgt ist. Die von Ihnen durchgeführten Aktionen werden dabei ausdrücklich nicht gespeichert. In beiden vorgenannten Fällen müssen Sie sich daher erneut mit Ihren Zugangsdaten am Wahlserver anmelden und die von Ihnen durchgeführten Aktionen wiederholen.

**Schutz vor Computerviren**

Ein Computervirus ist ein sich selbst vermehrendes Computerprogramm, das sich in andere Computerprogramme einschleust und sich damit reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion. Einmal gestartet, kann es von einer Benutzerin oder einem Benutzer nicht kontrollierbare Veränderungen am Status der Hardware (z.B. Netzwerkverbindungen), am Betriebssystem oder an der Software vornehmen (Schadfunktion). Computerviren können durch von der erstellenden Person gewünschte oder nicht gewünschte Funktionen die Computersicherheit beeinträchtigen. Installieren Sie daher einen Virenscanner auf Ihrem Computerarbeitsplatz und lassen Sie diesen regelmäßig alle Dateien auf Viren überprüfen (scannen). Achten Sie darauf, dass Sie ständig (täglich) die neuesten Aktualisierungen (Updates) einspielen, die alle führenden Herstellerfirmen von Virenscannern anbieten.

**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 von Ihnen unbemerkt an Dritte übertragen werden („Phishing“). Dadurch besteht das 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 begrenzten Schutz gegen derartige Trojaner können auch sogenannte „Anti-Spy-Programme“ bieten, die als lizenzierte, kostenpflichtige Produkte oder als Freeware (unentgeltlich nutzbare Computerprogramme) zur Verfügung stehen. Als Spyware wird üblicherweise Software bezeichnet, die persönliche Daten ohne Wissen oder Zustimmung von Nutzerinnen oder Nutzern eines Computers an Dritte sendet.

Darüber hinaus sollten Sie auch Software zur Fernwartung (z.B. TeamViewer) deaktivieren, um sicherzustellen, dass keine unbefugte Person den Wahlvorgang mitverfolgen kann und damit das Geheimnis der Wahl verletzt.

**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 Sie 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 ITZ: https://www.itz.uni-halle.de/dienstleistungen/sophos/

Weitere nützliche Tipps zum Thema Sicherheit im Internet erhalten Sie auch hier:
https://www.bsi-fuer-buerger.de

## 3. Hilfestellungen bei Problemen und Fragen

Für die Durchführung des Wahlvorgangs finden Sie im Löwenportal bzw. in der Ihnen per E-Mail oder Post zugegangenen Wahlbenachrichtigung eine schriftliche Kurzanleitung. Im Wahlsystem von Polyas werden Sie zudem Schritt für Schritt durch die Stimmabgabe mit Hinweisen und Erläuterungen durchgeleitet. Sollten Sie dennoch Fragen dazu haben, können Sie sich an das Wahlamt wenden. Dies gilt auch, wenn Sie eine sicherheitsrelevante Unregelmäßigkeit bemerken oder einen Verdacht auf Manipulation haben. In diesem Fall bitten wir um unverzügliche Information.

Sofern sich in Bezug auf Ihren persönlichen Computerarbeitsplatz technische Probleme oder Fragen ergeben sollten, wenden Sie sich bitte unmittelbar an die zuständigen IT-Verantwortlichen in Ihren Bereichen (Fakultät, Institut, Arbeitsgruppe) oder im Zweifel an den Helpdesk des ITZ.

**Kontakt**

Wahlamt der Martin-Luther-Universität Halle-Wittenberg
AnsprechpartnerIn:
Jana Fähling (Tel. 0345/55-21321)
Robert Felsch (Tel. 0345/55-21304)
orgawahlen@verwaltung.uni-halle.de
www.uni-halle.de/wahlen