Georg-August-Universität Göttingen
Sicherheitshinweise zu den digitalen Wahlen
im Wintersemester 2022/2023

I. Allgemeines

Die Wahlen an der Georg-August-Universität Göttingen zu den Kollegialorganen, zu den Studentischen Organen (inkl. Urabstimmungen), zur Klinikkonferenz (nur UMG) sowie zur Promovierendenvertretung werden im Wintersemester 2022/2023 als internetbasierte digitale Wahlen (im Folgenden: Onlinewahlen) mit Briefwahlmöglichkeit durchgeführt. Die Onlinewahl ist browserbasiert und betriebssystemunabhängig weltweit von EDV-Endgeräten ohne Installation einer Spezialsoftware möglich sowie einfach und intuitiv zu navigieren. Als technische Plattform wird das Wahlsystem POLYAS der POLYAS GmbH mit der auf die universitätsspezifischen Bedürfnisse angepassten Nutzerführung des Wahlsystems eingesetzt. An POLYAS wurde 2016 durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland erstmals das Zertifikat für eine Onlinewahl-Software erteilt und 2021 erneuert. Es basiert auf den Common Criteria für Onlinewahlen und dem Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, die sich aus den allgemeinen Wahlgrundsätzen ableiten. Dementsprechend sind Online-Wahlen in der Konfiguration Polyas CORE 2.5.3 und 2.5.4 nach Maßgabe der BSI-Anforderungen sicher und erfüllen die Ansprüche an das demokratische Wahlrecht.

II. Allgemeine Sicherheitshinweise

Die Abstimmung durch die Wahlberechtigten erfolgt bei den als Onlinewahl durchgeführten Wahlen auf einem individuell genutzten EDV-Endgerät mit Internetzugang (z.B. Arbeitsplatzrechner, Tablet, PC, Notebook, Smartphone), über welches die Stimmen verschlüsselt an das Wahlsystem übertragen werden.

Die Beachtung der hier empfohlenen Sicherheitsmaßnahmen soll sicherstellen, dass geeignete Vorkehrungen getroffen sind, um ein möglichst hohes Sicherheitsniveau zu gewährleisten und Angriffe durch „Computerviren, Würmer, Trojaner“ (im Folgenden: Schadprogramme) und ähnliche dienstebehindernde Attacken auf dem EDV-Endgerät und auf den Wahlservern zu verhindern sowie die persönliche Einhaltung des Wahlgeheimnisses zu gewährleisten.

Bitte beachten Sie auch die für alle Mitglieder und Angehörigen der Georg-August-Universität Göttingen (einschließlich UMG) geltende Informationssicherheitsrichtlinie (https://www.uni-goettingen.de/de/informationssicherheitssrichtlinie/52744.html).

III. Sicherheitstechnische Anforderungen an das EDV-Endgerät, das zur Durchführung der Wahl genutzt wird

Zur Durchführung des Wahlvorgangs ist ein übliches EDV-Endgerät mit funktionierendem Internetzugang erforderlich, wie es auch in den Einrichtungen der Georg-August-Universität und in vielen Privathaushalten üblich ist. Es wird angeraten, ausschließlich EDV-Endgeräte in vertrauenswürdigen Umgebungen zu nutzen, bei denen die grundsätzliche Einhaltung der empfohlenen Sicherheitsmaßnahmen im Allgemeinen sichergestellt wird. Diese Sicherheit wird z. B. in den Computerpools oder den Arbeitsplatzrechnern der Universität gewährleistet. Von der Nutzung von EDV-Endgeräten in nicht vertrauenswürdigen Umgebungen wird aus Sicherheitsgründen abgeraten. Wahlberechtigte sind grundsätzlich selbst dafür verantwortlich, dass die Beachtung der hier empfohlenen Sicherheitsmaßnahmen am genutzten EDV-Endgerät gegeben ist.

IV. Geheimhaltung der Zugangsdaten

Bitte achten Sie unbedingt darauf, dass Sie Ihre Zugangsdaten (Personal. bzw. Matrikelnummer und Passwort) sorgsam behandeln und unberechtigten Dritte keinen Zugriff auf diese Daten ermöglichen. Ihr Passwort halten Sie bitte unter Verschluss.

V. Einsatz von Computerprogrammen aus vertrauenswürdigen Quellen

Installieren und starten Sie keine Programme, die Sie von Unbekannten oder ungefragt von Bekannten per E-Mail oder aus anderen unsicheren Quellen erhalten haben. Vorsicht: Auch Bildschirmschoner sind Programme. Sofern auch nur geringe Zweifel an der Vertrauenswürdigkeit von Programmen bestehen, sollten Sie auf eine Installation auf Ihrem Rechner verzichten.

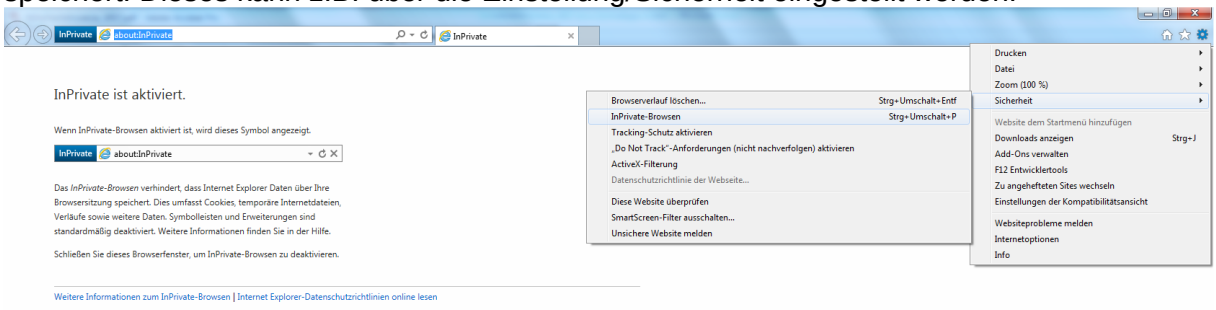
VI. Einstellungen der Browser

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 des Wahlsystems darauf verzichten, in einem zweiten Browser-Fenster andere Internetseiten mit nicht vertrauenswürdigen Inhalten anzuzeigen. Die Internetseiten des Wahlsystems 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. 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 sogenannte Cookies zum Speichern Ihrer persönlichen Einstellungen auf Webseiten nicht gespeichert werden.

Deaktivieren Sie die Funktion, welche Benutzernamen und Kennwörter für die automatische Eingabe bei späteren Aufrufen speichert. Sie finden diese Einstellungen häufig unter „Autovervollständigen“, oder sie heißen 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 EDV-Endgerät aufgerufenen Seiten nachträglich angesehen werden können. Sie können dafür zum Beispiel die Tastenkombination „Strg + Shift + Entf“ verwenden. Je nach Browser haben Sie dann die Möglichkeit, den Cache zu löschen.

Sie können die Browser aber auch im „Privaten Modus“ verwenden. Dabei nutzen Sie das Internet, ohne dass der Browser Daten über Ihre Webseitenbesuche auf Ihrem Rechner speichert. Dieses kann z.B. über die Einstellung/Sicherheit eingestellt werden.



VII. Sichere verschlüsselte Übertragung

Grundlage einer sicheren Internetverbindung ist die Verwendung eines sogenannten sicheren Protokolls für die verschlüsselte Übertragung der Daten (SSL oder 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 z.B. von Firefox und Mozilla durch ein geschlossenes Schloss-Symbol angezeigt. Bitte achten Sie darauf, dass nach der Anmeldung am Wahlsystem während der Verbindungsdauer dieses Symbol als „geschlossen“ dargestellt wird. Durch Doppelklick auf das jeweilige Symbol werden Ihnen weitere Informationen zum Sicherheitszertifikat angezeigt. Die Darstellung ist abhängig von der von Ihnen eingesetzten Browserversion. 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.

Als URL muss "https://election.polyas.com“ angezeigt werden. 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 (*polyas.com) hat folgende Fingerprints:

- SHA-1
  3D:E5:EA:28:A8:DB:54:82:04:9E:3F:A6:75:0F:FD:8C:94:BA:BA:F8

- SHA-256
  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

Sofern Sie diese Daten angezeigt bekommen, besteht eine sichere und verschlüsselte Verbindung zum Wahlsystem. Sollten Sie andere Daten angezeigt bekommen, beenden Sie die Verbindung sofort und informieren Sie bitte umgehend die Wahlleitung (die Kontaktdaten finden Sie insbesondere am Ende dieser Sicherheitshinweise, auf der Seite www.uni-goettingen.de/Wahlen, in der Wahlbenachrichtigung, in der Wahlausschreibung, in der Wahlbekanntmachung oder im Wahlsystem).

VIII. Nutzung des EDV-Endgeräts ohne administrative Rechte

Wir empfehlen dringend, das Internet (bzw. interne Netzwerke und externe Datenträger) nur mit einem Benutzer*innenkonto ohne Administrationsrechte zu nutzen; die universitären Accounts verfügen üblicherweise nicht über administrative Berechtigungen. Schadprogramme sind zur dauerhaften Installation auf fremden Rechnern meist darauf angewiesen, dass angemeldete Benutzer*innen über Administrationsrechte verfügen. Wie Sie ein solches Benutzungskonto ohne diese Rechte einrichten, können Sie der Dokumentation Ihres Betriebssystems entnehmen.

IX. Software zum Anzeigen von Internetseiten (Browser)

Zur Anzeige der im Internet (World Wide Web) angebotenen Informationen (Webseiten) werden spezielle Computerprogramme (Browser) zum Betrachten eingesetzt. Achten Sie darauf, dass Sie die eingesetzte Browser-Software aus vertrauenswürdigen Quellen bezogen haben, sodass sichergestellt ist, dass es sich um unveränderte Originalsoftware handelt. Bitte setzen Sie nur vom Hersteller freigegebene Versionen der Internet-Browser (Firefox, Mozilla, Opera, Safari, Edge etc.) ein. 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 Browser Ihres EDV-Endgeräts, z.B. für

Microsoft-Produkte mit Hilfe der Windows-Update-Funktion unter http://www.update.microsoft.com.

X. Einzelheiten zum Schutz vor Schadprogrammen

1. Schutz vor Computerviren

Ein Computervirus ist ein sich selbst vermehrendes Computerprogramm, welches 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 der*dem Benutzer*in 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.

2. 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 („Phising“). 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 Nutzer*innen 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 die Geheimheit der Wahl verletzt.

3. Überwachung des Datenverkehrs vom und zum Internet

Zusätzlichen Schutz vor Schadprogrammen, insbesondere „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 vom 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.

4. Bezugsquellen für Schutzprogramme

Für Mitglieder der Universität ist folgende Bezugsquelle zu empfehlen:

- https://antivir.gwdg.de/

Weitere Informationen und nützliche Tipps zum Thema Sicherheit im Internet erhalten Sie auch hier:

- http://www.bsi-fuer-buerger.de

XI. Nutzbarkeit des Wahlsystems trotz technischer oder persönlicher Einschränkungen

Die Wahlanwendung ist grundsätzlich für alle berechtigten Nutzer*innen unabhängig von deren körperlichen und / oder technischen Möglichkeiten weitgehend uneingeschränkt ohne besondere Erschwernis und in der allgemein üblichen Weise zugänglich und kann grundsätzlich ohne fremde Hilfe genutzt werden (barrierearm). 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.

XII. Wahlsystem

Bei der Onlinewahl kommt das Wahlsystem POLYAS der POLYAS GmbH (www.polyas.de) zum Einsatz. Das Wahlsystem 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 Onlinewahl das Internet genutzt. Die Kommunikation zwischen den Modulen erfolgt mittels des – als hinreichend sicher geltenden – Protokolls „https“ ausschließlich verschlüsselt. Daten, welche auf die persönliche Identität von Wahlberechtigten schließen lassen könnten, werden NICHT im Wahlsystem 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.

XIII. Autorisierung über einen universitären Benutzer*innen-Account

Die Wahlberechtigten melden sich mittels Eingabe der Personalnummer oder der Matrikelnummer und des Passworts (des Benutzer*innen-Account der Universität) über das Wahlportal der Universität unter https://onlinewahl.uni-goettingen.de/onlinewahl an. Nach der Anmeldung prüft das System, ob die*der Benutzer*in wahlberechtigt ist, und erzeugt daraufhin eine temporäre URL (SecureLink) zum Wahlsystem. Eine weitere Anmeldung am Wahlsystem ist nicht notwendig; die Wahlberechtigten können direkt mit der Stimmabgabe beginnen. Die Identität der*des Wählerin*Wählers ist geschützt.

XIV. Abmelden vom Wahlsystem / Automatische Zeitüberwachung /

Verlassen Sie das Wahlsystem bitte ordnungsgemäß über die Schaltfläche "Wahl abbrechen/ausloggen" (oben), wenn Sie den Wahlvorgang ab- oder unterbrechen wollen. Wenn Sie sich eingeloggt haben und für 15 Minuten inaktiv waren, werden Sie automatisch ausgeloggt. Dies dient der Sicherheit Ihrer Stimmabgabe; natürlich wird Ihre bisherige Stimmauswahl in diesem Fall nicht (zwischen)gespeichert wird. Sie können sich innerhalb des Wahlzeitraums erneut anmelden und digital wählen.

XV. Briefwahl

Bis zum 03. Januar 2022; 15:00 Uhr (Ausschlussfrist) konnte bei der Wahlleitung ein Antrag auf Briefwahl eingereicht werden. Mit dem Versand oder der Aushändigung der Briefwahlunterlagen sind die Wahlberechtigten von der Onlinewahl ausgeschlossen.

XVI. Hilfestellungen bei Problemen und Fragen

Für die Durchführung des Wahlvorgangs finden Sie über die Internetseite: www.uni.goettingen.de/wahlen Anleitungen oder Hilfestellungen. Für vertiefende Fragestellungen steht Ihnen darüber hinaus eine ausführliche Wahlanleitung online im Wahlsystem zur Verfügung.

Wenn Sie eine sicherheitsrelevante Unregelmäßigkeit, z.B. eine Manipulation, bemerken, wenden Sie sich bitte sofort an die Wahlleitung der Universität.

XVII. Kontaktinformationen

Sofern sich in Bezug auf Ihren persönliches EDV-Endgerät technische Probleme oder Fragen ergeben sollten, wenden Sie sich bitte unmittelbar an die Zuständigen für das Rechnernetz, an das das von Ihnen genutzte EDV-Endgerät angeschlossen ist.

Kontakt:

Wahlleitung der Georg-August-Universität Göttingen
Abteilung Wissenschaftsrecht und Trägerstiftung
Bereich 81
Von-Siebold-Straße 2
37075 Göttingen
https://www.uni-goettingen.de/wahlen
wahlen@uni-goettingen.de

Ansprechpartnerin:

Ralf Buhre
ralf.buhre@zvw.uni-goettingen.de
Tel. +49 551 39-28093