Exam Revision

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

02/04/2024
Exam Structure

• Three questions: you must do Question 1 and select either Question 2 or Question 3 to answer

• “NOTES PERMITTED, CALCULATORS NOT PERMITTED examination. Candidates may consult up to THREE A4 pages (6 sides) of notes. CALCULATORS MAY NOT BE USED IN THIS EXAMINATION”

• Past exams online: https://exampapers.ed.ac.uk/
Expectation

- Applying concepts and frameworks learned in the lecture
- Thinking and analyzing critically using logic and examples
  - What are the limitations/tradeoffs?
  - What are the experiment tasks and materials?
  - Any similar cases?
  - ...
- No statistics, calculation, and drawing tested in the exam
Topics

- USEC basics
- Study method and analysis
- Authentication
- Phishing
- Security and privacy communication (warning, advice, etc.)
- Privacy framework, tools, and policy
- Ethics and consent
- Access control, AI, IoT, at-risk users....
USEC Intro
## Defining security – CIA definition

<table>
<thead>
<tr>
<th>Security Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>No improper information gathering</td>
</tr>
<tr>
<td>Integrity</td>
<td>Data has not been (maliciously) altered</td>
</tr>
<tr>
<td>Availability</td>
<td>Data/services can be accessed as desired</td>
</tr>
<tr>
<td>Accountability</td>
<td>Actions are traceable to those responsible</td>
</tr>
<tr>
<td>Authentication</td>
<td>User or data origin accurately identifiable</td>
</tr>
</tbody>
</table>
Usability and human factors

- **Learn-ability** – The type for typical users to learn the actions relevant to a set of tasks.
- **Efficiency** – How long it takes users to perform typical tasks.
- **Errors** – The rate of errors users make when performing tasks.
- **Memorability** – How users can retain their knowledge of the system over time.
- **Subjective satisfaction** – How users like the various aspects of the system.
USEC is challenging because

• Interdisciplinary
• Seemingly familiarity
• Interrelations
• User evaluation
• Ecological validity
• Adversary model
• Technology velocity
• Customer
Threat Modelling: Adversaries

• Malicious actors
  • Hacker
  • Users (your family, your friend, your customer, etc.)
• Service providers
  • Company
  • App developers
• “Big brother”
• ... (depending on your position)
Assets

• Computer hardware: phone, laptop, server...
• Computer software: apps, operating systems, database...
• Physical assets: house, car.....
• Information: health record, your profile/identity, business info...
• Emotion, reputation, user experience....
Risk, threat and vulnerability

- Vulnerability: the weakness of X (system/human) that can be exploited
  - The program is overprivileged to access things
  - The user reuses their password across applications
- Threat is an action performed by the adversary to damage the asset by exploiting a vulnerability
- Risk = asset X threat X vulnerability
Study and Analysis Methods
Project lifecycle

1. What is wanted / needed
2. Analysis
3. Design
4. Implement and deploy
5. Prototype

The diagram shows a flow from What is wanted / needed to Analysis, then to Design, to Implement and deploy, and back to Prototype, indicating a cyclical process.
Ethics guidelines

School of Informatics Intranet
INFWEB

Ethics procedure

An overview of the School's ethics procedure, including when and how to complete an ethics application for review.

Consideration of the ethical aspects of our research is both a moral and a legal obligation, as well as part of the academic culture in which we should be training researchers. The following procedures should help us fulfill those requirements. The goal of the system is full legal accountability with minimal effort. The first goal is served by keeping the full record. The second goal is served by keeping form filling to a minimum, by holding information locally, and by assuring that decision-making is as close to the pertinent research expertise as possible.

The procedures proposed here aim to ensure that ethical consideration are taken into account in any research done in the School. The proposed framework borrows heavily from current practice in PPLS Psychology and Linguistics, as well as procedures in GeoSciences.

The system outlined on these pages apply to UG final year projects, MSc projects, PhD projects, Post-doc fellowships, funded research requiring a proposal, research performed by a visitor, and personal research for which there is no proposal.

Ethics application via online form

This is the online form, which has replaced the old Word forms. Please use it for all staff and student projects. Your data is stored on a server in the EU, following UK GDPR rules. The Principal Investigator will receive a copy of the form.

If you are submitting more than one ethics application, please wait to receive the automated confirmation of receipt for your first application before submitting the next.

Once submitted, the panel will aim to reply within 10 working days.

Update for December 2023 / January 2024:
Ethics guidelines

Level 1
Reviewed by one assigned member of the Informatics ethics committee
Applications are considered at level 1 if the proposed research involves human participants or personal data, but it does not involve any of the points outlined under level 2.

Level 2
Reviewed by two assigned members of the Informatics ethics committee
Applications are considered at level 2 if the research involves any of the below:

- Issues with regards to the safeguards quoted as good practice in the University’s Data Protection policy (including the minimization principle, anonymization of personal data, and secure storage of data. See the University’s data protection policy and accompanying handbook for further information (sections 12 and 13 relevant for research and student projects respectively).
  - Data Protection Policy
  - Data Protection Handbook

- Issues with regards to data protection and consent, including but not limited to:
  - The use of services which are not UK GDPR compliant (e.g. Dropbox) to store data that are sensitive and/or could be used to identify participants.
  - The collection of participant data without explicit participant consent (e.g. where participants cannot meaningfully provide consent [see also Vulnerable participants]), or where administrative consent is sought in lieu of participant consent (e.g. for aggregated information on participants)

- Significant potential for physical or psychological harm, discomfort or stress, including but not limited to:
  - Projects where the true purpose of the research is concealed from participants
  - Potential harm to the researcher(s)

- Vulnerable participants, including but not limited to individuals who are:
  - under the age of 15
  - disabled
  - in any other dependent relationship with the researcher(s), e.g. student-teacher
  - known to have special education needs
  - physically or mentally ill, or with diminished cognitive capacity
  - in the care of a Local Authority

https://uoe.sharepoint.com/sites/inf-researchservices/SitePages/Ethics-levels.aspx
Behavioral – measures how people actually behave, what they do.

Attitudinal – measures what people say they think or how they say they behave.
Qualitative – unstructured data such as natural language.

Quantitative – numerical data. Anything that can be counted or measured with numbers.
Lab Study

• Basic idea: Have a participant come to a physical place (lab) and interact with the interface there
• You setup the lab so it mimics the situation you want to test
• Pros
  • Full control over the environment so limited confounds
  • Detailed data from each subject
  • Ability to ask them why they did something
• Cons
  • Small sample sizes
  • Being in the lab changes user behavior. They feel safer and their normal distractions are gone. That can be bad for deception studies.
Think aloud

- Basic idea: Have a participant use the interface and speak aloud while they do so
- Think aloud is a very versatile, can be long or short, detailed or minimal, planned or ad-hoc
- Pros
  - Learn what the user is trying to do and why they click on some things
  - Very detailed information
  - Testing with about 5 users will find the majority of major (usability) issues
- Cons
  - Biasing user behavior, making the situation unnatural
  - (Concurrent) Talking aloud changes how long a user spends on tasks so this method cannot be combined with timing

https://www.nngroup.com/articles/thinking-aloud-the-1-usability-tool/
Survey scales

• Basic idea: A set of questions that have been previously shown to measure a property.

• Pros

  • Easy to copy-and-paste into a survey.
  • Allows you to measure hard-to-measure concepts like risk seeking behavior or attitude towards privacy.

• Cons

  • Making a new scale is very challenging.
  • Can contain an annoyingly large number of questions.
Planning a survey

• Surveys normally answer **multiple research questions**. With each research question tied to one or more survey questions.

• **Descriptive** – learn something about the whole population.
  • How many people have heard of the term “phishing”?
  • What words do people use to describe cookie tracking?

• **Testing for correlation or causation** – show that two things are related or one thing causes the other thing.
  • If someone has been trained on phishing in the past, are they better at differentiating phishing emails?
  • We have three training options, each user goes through one training, which training causes people to identify phishing emails the best?
Testing: Correlation vs. Causation

• Correlation
  • Two things tend to behave in a way that seems inter-related, where if one thing changes the other thing will also change in a related way.
  • For example, if the price of rice goes up at the same time as the price for beans.

• Causation
  • When one thing changes it causes the other thing to change.
  • For example, when the weather gets cold more people wear coats. Cold weather causes more people to wear coats.
Testing: What are you going to measure?

• In statistics there are classically two types of measurements (variables): dependent and independent

• Dependent
  • Also known as the **outcome variable**
  • “Dependent” on the study
  • Measures the usability **goal**

• Independent
  • Anything **you are directly manipulating**
  • An element of the study which is under your control
  • A pre-existing feature of your participant
Testing: Between vs. Within subjects

• **Between subjects**
  • Your study only shows one interface to one person
  • You are measuring how well the people randomly assigned to the A interface did compared to the people randomly assigned to the B interface
  • **Lots of variability with this method**

• **Within subjects**
  • Your study shows all interfaces to all people
  • You are measuring the difference in how they do on the two interfaces
  • **Less variability (same person) but more learning effects and priming**
Testing: Types of data

• Numeric
  • **Continuous** – Any value on the range is possible including decimal (1-5)
  • **Discrete** – Only certain values on the range are possible (1,2,3,4,5)
  • **Interval** – Only certain values on the range are possible and each has equal distance from its neighboring values (strongly agree, agree, neutral, disagree, strongly disagree)

• Categorical
  • **Binary** – Only two possibilities (true, false)
  • **Ordinal** – The values have an ordering (slow, medium, fast)
  • **Nominal** – The values have no ordering (apple, pear, kiwi, banana)
Some research questions:

- Can people differentiate between a subdomain and a domain when reading a URL?
- Does [my new system] help people differentiate between malicious URLs and safe ones?
- Can users use [my new password manager] faster and with less errors than [the old password manager]?
- Does knowing how an app will use its permissions impact app installation decisions?
- What factors impact end-users’ willingness to update software?
- Using [website], can users successfully opt-out of cookie tracking without forming inaccurate mental models?
Study design

- RQ: Does [my new interface] enable people to accurately determine what permissions an app will use?
- A/B test between the existing and new interface
- Between subjects
- 10 Tasks shown in the same order to all participants
- Dependent variables
  - Accuracy on task
- Independent variables
  - Which interface (A or B)
Inductive coding vs deductive coding

- **Inductive (bottom-up):** look for any ideas that interest you from different aspects
  - Snapshot of an app on a phone
  - Child playing with dog
  - Edited picture
  - Motion detection enabled
  ...

- **Deductive (top-down):** start with some hypothesis
  - Children being monitored by app (privacy concern)
  - Camera placed in the living room (place of the scene)
6 Steps to Doing a Thematic Analysis

**STEP 1**
Gather your data.

**STEP 2**
Read all your data from beginning to end.

**STEP 3**
Code the text based on what it’s about.

**STEP 4**
Create new codes to encapsulate potential themes.

**STEP 5**
Take a break for a day.

**STEP 6**
Evaluate your themes for good fit.

**REPEAT AS NEEDED**
Framework and Topics
Human in the Loop Framework

https://medium.com/@ezgineer/usable-security-and-privacy-introduction-d676abc8c61d
Other Frameworks: What are they used for and how to use them?

• NEAT
• SPRUCE
• Privacy by design
• Contextual integrity
• ....
A TAXONOMY OF PRIVACY

INFORMATION PROCESSING

AGGREGATION
Combining of various pieces of personal information
A credit bureau combining an individual’s payment history from multiple creditors

SECONDARY USE
Using personal information for a purpose other than the purpose for which it was collected
The U.S. Government using census data collected for the purpose of apportioning Congressional districts to identify and retain those of Japanese descent in Hawaii

EXCLUSION
Failing to let an individual know about the information that others have about them and participate in its handling or use
A company using customer cell history without the customer’s knowledge, to shift their order in a queue (i.e. “Your call will be answered in the order [NOT] received”)

INSECURITY
Failing to protect information
An ecommerce website allowing others to view an individual’s purchase history by changing the URL (e.g., abc@privacy.com/?id=123)

IDENTIFICATION
Linking of information to an individual. [Sometimes called “slinging out”]
A researcher linking medical files to the Governor of a state using only state of birth, zip code and gender

COLLECTION

SURVEILLANCE
Watching, listening to, or recording of a person’s activities
A website monitoring cursor movements of a visitor while visiting the website

INTERROGATION
Questioning or probing for personal information
An interviewer asking an inappropriate question, such as marital status, during an employment interview

INVASION

INTRUSION
Disturbing a person’s tranquility or solitude
An augmented reality game directing players onto private residential property

DECISIONAL INTERFERENCE
Intruding into a person’s decision making regarding their private affairs
A payment processor deciding transactions for contraceptives

INFORMATION DISSEMINATION

DISCLOSURE
Revealing truthful information about a person that impacts their security or the way others judge their character
A government agency revealing an individual’s address to a stalker, resulting in the individual’s murder

EXPOSURE
Revealing a person’s nudity, grief, or bodily functions
A store forcing a customer to remove clothing revealing a colostomy bag

BREACH OF CONFIDENTIALITY
Breaking a promise to keep a person’s information confidential
A doctor revealing patient information to friends on a social media website

INCREASED ACCESSIBILITY
Amplifying the accessibility of personal information
A court making personal information searchable on the Internet without redacting personal information

APPROPRIATION
Using an individual’s identity to serve the aims and interests of another
A social media site using customer’s images in advertising

DISTORTION
Disseminating false or misleading information about a person
A credit report reporting a paid bill as unpaid to a credit bureau

Version 6 (2022)
https://privacybydesign.training
Privacy by design – strategies
Contextual integrity

https://www.dli.tech.cornell.edu/post/privacy-policies-as-contextual-integrity-beyond-rules-compliance
Authentication

What you know

What you have

Who you are
A good authentication method:

**User friendly**
- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

**Reasonable to implement**
- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

**Protects against attacks**
- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable
Attributes of a “good” biometric feature

1. **Universality**: Does everyone have it?
2. **Distinctiveness**: Is it different for everyone?
3. **Permanence**: Does the feature change over time/age?
   - bad: face, good: fingerprint
4. **Collectability**: How easy it is to collect/measure the feature?
   - Very hard: DNA, relatively easy: fingerprint
5. **Performance**: How difficult to match?
6. **Acceptability**
7. **Circumvention**: How easy to spoof?
   - Voice recognition

The Phishing Ecosystem

- Phisher
- List of known phishing sites
- Volunteer
- Web servers
- Potential phishing sites
- Email server
- Fake login
- Web browser
- Trash
- Report
- End user
- More potential victims
- Local rules
- University
- ISP
- Bank
- Help desk

End User

Phisher

List of known phishing sites

Volunteers

Web servers

Potential phishing sites

Email server

Fake login

Trash

Report

End user

More potential victims

Local rules

University

ISP

Bank

Help desk
Common phishing elements

• **Automated** – Typically directed against many people.

• **Impersonation** – Communication claims to be from someone trusted or that they are not. For example, from a bank.

• **Direction to a website** – Links that look like they go somewhere legitimate but in fact go somewhere controlled by the attacker.

• **Contain an attachment** – Attachment asks for information to be sent back or contains malicious code.

• **Authentication info requested** – The communication aims to get authentication information.
Main “solutions” against phishing

- Automatically block attacks using filters
- Train users
- Support users
- Improve protection of authentication credentials
NEAT

**Necessary** – Can you change the architecture to eliminate or defer this user decision? Interrupt users only when necessary.

**Explained** - Does your user experience present all the information the user needs to make this decision? Explain the decision users need to make with information *(See SPRUCE)*

**Actionable** – Have you determined a set of steps the user will realistically be able to take to make the decision correctly? Give steps in all scenarios (e.g., benign vs malicious)

**Tested** – Have you checked that your user experience is NEAT for all scenarios, both benign and malicious? Have you tested it on a human who is not a member of your team? Do usability testing.
**SPRUCE**

**Source** – State who or what is asking the user to make a decision

**Process** – Give the user actionable steps to follow to make a good decision

**Risk** – Explain what bad thing could happen if they user makes the wrong decision

**Unique** – Knowledge the user has – Tell the user what information they bring to the decision regarding the context

**Choices** – List available options and clearly recommend one

**Evidence** – Highlight information the user should factor in or exclude in making a decision
## Privacy space framework

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness</td>
<td>Informative</td>
<td>Display information about trackers on current webpage, whether location is being sent</td>
</tr>
<tr>
<td>Detection</td>
<td>Actively look for problems</td>
<td>Find trackers on current webpage</td>
</tr>
<tr>
<td>Prevention</td>
<td>Used as a precaution</td>
<td>Encryption tools, anonymity tools</td>
</tr>
<tr>
<td>Response</td>
<td>Taking action after a problem is detected</td>
<td>Tracking blocker</td>
</tr>
<tr>
<td>Recovery</td>
<td>Help you get back to normal</td>
<td>Patching bugs</td>
</tr>
</tbody>
</table>

All sorts of things need to be communicated to users

- **Questions** – “did you log in from this location?”
- **Warnings** – “the website has malicious software”
- **UI passive indicators** – the lock icon on the browser
- **UI active indicators** – “You need to generate a key”
- **Task-relevant information** – “Passwords should be 8 characters long and must have a capital letter.”
- **Educational** – “10 security behaviors you should do to protect yourself online”
- **Awareness** – “This phishing email has been going around, don’t fall for it.”
## Access Control Matrix

### Objects (files)

<table>
<thead>
<tr>
<th>Subjects (users)</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>jingjie</td>
<td>r,w</td>
<td>-</td>
<td>r,w, own</td>
<td>-</td>
<td>r</td>
</tr>
<tr>
<td>bob</td>
<td>-</td>
<td>-</td>
<td>r</td>
<td>r</td>
<td>r,w</td>
</tr>
<tr>
<td>alice</td>
<td>w, own</td>
<td>r</td>
<td>r</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>eve</td>
<td>r</td>
<td>r,w</td>
<td>r,w</td>
<td>-</td>
<td>r</td>
</tr>
</tbody>
</table>

[Source: Lampson, Graham, Denning; 1971]

Could be a very huge table to store and access!

<table>
<thead>
<tr>
<th>Principle</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respect for Persons</td>
<td>Participation as a research subject is voluntary, and follows from informed consent; Treat individuals as autonomous agents and respect their right to determine their own best interests; Respect individuals who are not targets of research yet are impacted; Individuals with diminished autonomy, who are incapable of deciding for themselves, are entitled to protection.</td>
</tr>
<tr>
<td>Beneficence</td>
<td>Do not harm; Maximize probable benefits and minimize probable harms; Systematically assess both risk of harm and benefit.</td>
</tr>
<tr>
<td>Justice</td>
<td>Each person deserves equal consideration in how to be treated, and the benefits of research should be fairly distributed according to individual need, effort, societal contribution, and merit; Selection of subjects should be fair, and burdens should be allocated equitably across impacted subjects.</td>
</tr>
<tr>
<td>Respect for Law and Public Interest</td>
<td>Engage in legal due diligence; Be transparent in methods and results; Be accountable for actions.</td>
</tr>
</tbody>
</table>
The basic requirements for the effectiveness of a valid legal consent are defined in Article 7 and specified further in recital 32 of the GDPR. Consent must be freely given, specific, informed and unambiguous. In order to obtain freely given consent, it must be given on a voluntary basis. The element “free” implies a real choice by the data subject....
Some ethical practices for social media research

- Follow the terms of use
- Obtain informed consent when possible
- Check our ethics guidelines for more!
### Safe practices for at risk users

<table>
<thead>
<tr>
<th>Category</th>
<th>ID</th>
<th>Digital-safety practices</th>
<th>Example papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional partnerships &amp; Ethical review</td>
<td>SP1</td>
<td>Elicit expert (academic) opinion on topic area</td>
<td>[17, 31, 67, 70, 82, 83, 112, 132, 136]</td>
</tr>
<tr>
<td></td>
<td>SP2</td>
<td>Form professional partnerships (e.g., support services for at-risk users)</td>
<td>[44, 52, 72, 80, 82, 99, 105, 124, 134, 145]</td>
</tr>
<tr>
<td></td>
<td>SP3</td>
<td>Invite and include an at-risk user to join research team</td>
<td>[17, 83, 97, 112]</td>
</tr>
<tr>
<td></td>
<td>SP4</td>
<td>Seek external (non-institutional) ethical review approval or monitoring</td>
<td>[30, 43, 44, 78]</td>
</tr>
<tr>
<td>Positionality &amp; Participant engagement</td>
<td>SP5</td>
<td>Build rapport with participants for understanding digital-safety needs</td>
<td>[1, 33, 34, 38, 73, 91, 97, 113, 137]</td>
</tr>
<tr>
<td></td>
<td>SP6</td>
<td>Conduct pilot studies with general (non-at-risk) users</td>
<td>[5, 30, 33, 64, 67, 95, 101]</td>
</tr>
<tr>
<td></td>
<td>SP7</td>
<td>Conduct studies with proxies for at-risk users (e.g., advocacy groups)</td>
<td>[2, 24, 33, 70, 74, 104, 132]</td>
</tr>
<tr>
<td></td>
<td>SP8</td>
<td>Include researchers whose identities affirm participants’</td>
<td>[2, 6, 38, 64, 97, 110, 112, 113, 132, 134]</td>
</tr>
<tr>
<td></td>
<td>SP9</td>
<td>Practice responsiveness in data collection sessions to potential threats</td>
<td>[3, 38, 49, 89, 100, 101, 124, 127, 128, 132]</td>
</tr>
<tr>
<td></td>
<td>SP10</td>
<td>Provide professional therapeutic support for emotive topics</td>
<td>[7, 11, 30, 48, 95, 100, 101, 115, 144]</td>
</tr>
<tr>
<td></td>
<td>SP11</td>
<td>Train team members in working with digital-safety risks</td>
<td>[7, 38, 115, 121]</td>
</tr>
<tr>
<td>Privacy-preserving data collection</td>
<td>SP12</td>
<td>Discourage participant self-disclosure (e.g., personal histories)</td>
<td>[1, 7, 25, 52, 70, 75, 78, 118, 123, 137, 144]</td>
</tr>
<tr>
<td></td>
<td>SP13</td>
<td>Focus data collection on supporting participant safety needs</td>
<td>[24, 34, 38, 66, 81, 97, 120, 121, 123, 129]</td>
</tr>
<tr>
<td></td>
<td>SP14</td>
<td>Do not collect or ask for participant demographic data</td>
<td>[17, 26, 64, 83, 84, 104, 120, 124, 136, 145]</td>
</tr>
<tr>
<td></td>
<td>SP15</td>
<td>Do not collect personally identifiable information on participants</td>
<td>[30, 43, 44, 52, 54, 58, 73, 85, 95, 143]</td>
</tr>
<tr>
<td></td>
<td>SP16</td>
<td>Implement protocols for researchers to prevent stalking by adversaries</td>
<td>[30, 60, 80]</td>
</tr>
<tr>
<td></td>
<td>SP17</td>
<td>Separate potential threats from at-risk users during data collection</td>
<td>[6, 72, 88, 96, 97, 100, 110, 115]</td>
</tr>
<tr>
<td></td>
<td>SP18</td>
<td>Permit participants to contribute false information (e.g., pseudonyms)</td>
<td>[17, 54, 58, 78, 83, 100]</td>
</tr>
<tr>
<td></td>
<td>SP19</td>
<td>Offer participants many modalities to contribute (e.g., audio, notes)</td>
<td>[4, 7, 24, 34, 57, 67, 90, 107, 117, 130]</td>
</tr>
<tr>
<td></td>
<td>SP20</td>
<td>Secure confidentiality and privacy of online and in-person research sites</td>
<td>[6, 24, 30, 43, 44, 77, 100, 113, 134, 139]</td>
</tr>
<tr>
<td>Secure data storage &amp; processing</td>
<td>SP21</td>
<td>Implement strict data access control measures for research data</td>
<td>[1, 7, 34, 51, 80, 112, 134, 136, 139, 147]</td>
</tr>
<tr>
<td></td>
<td>SP22</td>
<td>Redact participant information prior to analysis by research team</td>
<td>[59, 86, 95, 107, 114, 128, 130, 140, 143, 156]</td>
</tr>
<tr>
<td></td>
<td>SP23</td>
<td>Use encryption for research data in-transit and at-rest</td>
<td>[52, 60, 75, 85, 86, 87, 101]</td>
</tr>
<tr>
<td></td>
<td>SP24</td>
<td>Use non-encrypted safe storage for research data in-transit and at-rest</td>
<td>[7, 30, 34, 90, 97, 114, 130, 132]</td>
</tr>
<tr>
<td>Researcher accountability</td>
<td>SP25</td>
<td>Conduct data collection sessions around participant schedules</td>
<td>[1, 35, 54, 65, 97, 111, 120, 128, 139]</td>
</tr>
<tr>
<td></td>
<td>SP26</td>
<td>Offer formal proof of identity as professional researchers</td>
<td>[70, 82, 97, 112, 114, 115]</td>
</tr>
<tr>
<td></td>
<td>SP27</td>
<td>Only use data from publicly accessible sites (e.g., no authorization)</td>
<td>[11, 32, 40, 97, 103, 138, 147, 155]</td>
</tr>
<tr>
<td></td>
<td>SP28</td>
<td>Provide proportional incentives to participants for contributions</td>
<td>[54, 64, 72, 73, 82, 110, 114, 134, 139, 145, 151]</td>
</tr>
<tr>
<td></td>
<td>SP29</td>
<td>Be transparent with participants about risks incurred by research</td>
<td>[24, 26, 38, 54, 57, 69, 95, 110, 113, 126]</td>
</tr>
<tr>
<td>Sharing &amp; evaluating deliverables</td>
<td>SP30</td>
<td>Do not attribute reported data contributions with participant identifiers</td>
<td>[7, 8, 9, 34, 55, 84, 114, 117, 134]</td>
</tr>
<tr>
<td></td>
<td>SP31</td>
<td>Do not report participant demographics in research deliverables</td>
<td>[17, 24, 43, 77, 78, 83, 117, 120, 144, 145]</td>
</tr>
<tr>
<td></td>
<td>SP32</td>
<td>Do not report participant names, pseudonyms, or identifiers</td>
<td>[9, 48, 71, 78, 101, 114, 121, 143, 145, 155]</td>
</tr>
<tr>
<td></td>
<td>SP33</td>
<td>Paraphrase or withhold sources of data (e.g., websites they use)</td>
<td>[2, 9, 17, 40, 59, 69, 78, 123, 136, 155]</td>
</tr>
<tr>
<td></td>
<td>SP34</td>
<td>Evaluate research deliverables for adversarial feedback or education</td>
<td>[34, 38, 44, 59, 82, 113]</td>
</tr>
<tr>
<td></td>
<td>SP35</td>
<td>Selectively edit participant data in research deliverables</td>
<td>[7, 9, 11, 40, 55, 124, 139, 140, 150, 151]</td>
</tr>
<tr>
<td></td>
<td>SP36</td>
<td>Provide participants control of their contributions (e.g., permit redaction)</td>
<td>[7, 47, 54, 75, 91, 113, 117, 136]</td>
</tr>
</tbody>
</table>
# Safe practices for at risk users

<table>
<thead>
<tr>
<th>ID</th>
<th>Strategy title</th>
<th>Description</th>
<th>Example digital-safety practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>Engage experts early</td>
<td>Consult or partner with domain experts from the beginning to inform and help facilitate safe research plans.</td>
<td>SP1, SP2, SP3, SP4, SP10</td>
</tr>
<tr>
<td>S2</td>
<td>Assess and mitigate risks by threat modeling</td>
<td>Apply the S&amp;P practice of threat modeling to research protocols, and continuously update threat models to guide ongoing safety mitigations.</td>
<td>SP11, SP16, SP17, SP20</td>
</tr>
<tr>
<td>S3</td>
<td>Select the lowest risk method that addresses the research goals</td>
<td>Before soliciting at-risk users for high-touch methods like interviews, consider proxies (e.g., advocates), or indirect methods (e.g., online measurement).</td>
<td>SP6, SP7, SP12, SP14, SP15, SP27</td>
</tr>
<tr>
<td>S4</td>
<td>Respect that at-risk users self-manage risk</td>
<td>At-risk users are often experts in managing their safety risks. Give them choice in how they engage with research safety protocols, and respect the choices they make.</td>
<td>SP9, SP18, SP19, SP25, SP26, SP29</td>
</tr>
<tr>
<td>S5</td>
<td>Be an advocate for at-risk users’ needs</td>
<td>Research, by its nature, can be extractive. Build reciprocity with at-risk users, and work to help them achieve their goals.</td>
<td>SP5, SP8, SP13, SP28, SP36</td>
</tr>
<tr>
<td>S6</td>
<td>Handle data and publications carefully</td>
<td>Data collection and analysis should follow security best-practice, and publications should avoid revealing identities or informing adversaries.</td>
<td>SP21, SP22, SP23, SP24, SP30, SP31, SP32, SP33, SP34, SP35</td>
</tr>
<tr>
<td>1998 Act:</td>
<td>GDPR:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle 1 – fair and lawful</td>
<td>Principle (a) – lawfulness, fairness and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>transparency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle 2 – purposes</td>
<td>Principle (b) – purpose limitation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle 3 – adequacy</td>
<td>Principle (c) – data minimisation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle 4 – accuracy</td>
<td>Principle (d) – accuracy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle 5 - retention</td>
<td>Principle (e) – storage limitation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle 6 – rights</td>
<td>No principle – separate provisions in</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chapter III</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle 7 – security</td>
<td>Principle (f) – integrity and confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle 8 – international</td>
<td>No principle – separate provisions in</td>
<td></td>
<td></td>
</tr>
<tr>
<td>transfers</td>
<td>Chapter V</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(no equivalent)</td>
<td>Accountability principle</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>