Welcome to The Tor Project!

Intro spiel

- Get people excited about the fact that they now work in Tor.
- Speak about how working for Tor is awesome

Getting set up

The Tor project uses a centralized user management system, userdir-ldap, to manage access to all torproject.org hosts and to manage @torproject.org e-mail forwarding.

Getting an account

If you are a contractor or employee then chances are your account already has been created by the time you read this.

If you are a volunteer or your account has not been created yet,system administrators can make an account for you. For the the instructions at https://help.torproject.org/tsa/doc/accounts/.

Using your account

Once your account is set up, you can get email forwarding via your <username>@torproject.org address to the address you specified during account creation. If you ever want to change that destination address, either:

- Log into https://db.torproject.org/ to update your information, or
- Send a PGP-signed message to changes@db.torproject.org. Read the instructions at

https://db.torproject.org/doc-mail.html to learn which email attributes you can change and how to change them.

Setting up ssh keys

You must set ssh authentication keys for your account in order to work with Tor code. Simply send a PGP-signed message containing one or more of your public ssh keys to changes@db.torproject.org. Since a lot of mail infrastructure breaks clear signed messages, we recommend using *gpg --armor --sign* and mailing the resulting base64 encoded blob.

Note that you can have more than one ssh key, but they all have to be submitted at the same time in on message. After you send your key(s), there will be a short delay (up to 20 minutes) before the information gets replicated to all hosts.

Accessing Git

Tor uses Git for software version control. To access our read-write Git repositories, you must have previously set up your ssh key(s). This will give you access the repositories under ssh://git@git-rw.torproject.org/. If running *ssh git@git-rw.torproject.org* gives you a permission denied error, you probably haven't yet set up your keys correctly.

Once you're on Git, you can see Tor's repositories, and which, if any, special privileges you have on them.

To get access to an existing repository please ask a person who already has access to file a ticket requesting you be given access.

To clone a repository, use the *user@server:path/to/repo.git* format. For example to clone the tor repository, you would enter *git@git-rw.torproject.org:tor*.

If you require a new personal repository under /user/<username>, please file a ticket in the corresponding trac category. See https://trac.torproject.org/projects/tor/wiki/org/operations/Infrastructure/git.torproject.org for instructions.

Accessing other ssh resources

By default all accounts are in the torproject group. Membership in this group gives access to the hosts lemmonii and perdulce.

lemmonii.torproject.org is a general purpose shell host. If you want to try things or run the occasional script from cron then this is probably the host to use. Several people also use it to run a persistent chat client to connect to our IRC channels.

perdulce.torproject.org is the personal web-page host. If you create a public_html directory in your home directory on perdulce then anything below that will be accessible as https://people.torproject.org/~<username>/. Please ensure that anything you put there is distributable, either created by you or properly licensed under a license that gives us permission to distribute it.

Accessing other hosts

If you want to help maintain a service that runs on a particular host you probably just need to get added to the relevant unix group. Again ask somebody who already has access to file a ticket on your behalf. See https://help.torproject.org/tsa/doc/accounts/ and https://trac.torproject.org/projects/tor/wiki/org/operations/Infrastructure for more information.

Op sec instructions

- Border crossing
- Backups are important

Communication

- Expectations for communication
- Mailing lists
- IRC
- Dev Meetings - who goes? what's the purpose?
- Trac
- Jabber/XMPP

Accounting and admin stuff

- Trip reports and status reports
- Travel
- Timesheets
- contracts
- Point of contact for admin related issues
- In which circumstances your income gets disclosed by name.

Dev ops

- Instructions on using gitweb
- Code review
- How to use trac
- How do a maintain a product, a service

Contacts

- List of tor people contacts and prioritized on the preferred means of contact

Culture of Tor

- Do-ocracy organizational structure
- Elitist approach and state that we are not actually like that
- Questions are welcome, etc.
- Importance of constructive criticism

Deliverables

- How do I interact with deliverables?
- How do they get negotiated?

- When should I bill?

External relationships

- How to do training material
- Requests for Information, Interviews, etc. from the Press Community:

A. Highly Public Situations: For highly public events our process will be to put together a general statement from Tor which will be the first point of contact to direct the press to - this will help us respond quickly and give them information to think until they figure out what else they need from us. This statement and follow up blog posts will FIRST be sent to tor-internal for comments/review/or additional key information which will help us offset any problems. This request through tor-internal will have a specific "by when" date when feedback is needed back and a date/time when the statement will go live. In the past this statement was reviewed by execdir and Andrew before posting - we are now extending this review to tor-internal to keep everyone in the loop. In addition, during times like this week many people want to have a phone or in person interview with a member of the Tor team - in those instances we try our best to accommodate using the people on execdir, Jake and Nick - as they are available.

B. Getting a Request Directly: If members of the Tor team receives a request directly please forward it to execdir -please provide (email or phone call) all key information that will help us understand who this person is, why they contacted you, any recommendations on responses, etc. The more information you provide the easier it is for us to respond quickly, knowledgeably and consistently - with only pieces of information we are putting ourselves at risk to respond inaccurately. Karen, Andrew or myself will response and commit to "cc" the Tor person who forwarded is kept in the loop. Also, please know we are keeping a list of where requests are coming in from the press - this helps us to manage a history of people in the press we trust, who put Tor in the best light and a get sense of what messages we have put in front of them in the past and what they did with them (for example, did they twist everything we said). Last - "cc"ing the Tor member who sent the request has always been our process however, if at any point this was not done during the influx of requests this week and if anyone felt "out of the loop", I apologize.

C. Additional Information Needed: there will be occasions where we get requests from the press which are technical or because of the complexity of the question we would like additional information for all you since you are closest to the technology and the people using Tor. Please know, if this information is needed it will be sent out via tor-internal for comment and input. It will have a clear "by when" date for people to comment/respond. Please know the "by when" dates we will put out when making these request are important for us to then flow information back out to the press.

Messaging for Current Events:
We wanted to share with all of you the key message points execdir has been and will continue to use on in our interactions with the press and media community about the current situation.

The focus of all of our responses to the press in general include:

- We are experts in privacy and anonymity our work is focused on privacy and anonymity - all the usual points made via our website, presentations and annual report;
- In our interactions with the media we will focus on examples which present Tor in the most positive light - doesn't have to be kittens and rainbows, but positive uses of Tor where we can help to make us look less scary when people are already nervous;
- Spotlight trainings, learning and speaking events where members of the Tor team are out in the world helping to educate people about privacy and anonymity;
- We work with a lot of people doing good in the world to help them not only understand Tor but also the large privacy landscape - and we hand out a lot of stickers along the way.

- Fundraising
- Best practices for talking about Tor - the points below are
    - The Tor Project is a nonprofit 501(c)(3) organization dedicated to providing tools to help people manage their privacy on the Internet.
    - Tor is a technology and research company - it is important to remember that technology is agnostic and that the moral compass of good or evil is in the human using the technology, not the technology itself. Tor will remain content neutral because we have to, both by design and morally.
    - Bad actors use email, cell phones, web browsers, web forums, twitter, instant messaging, Skype, Facebook, and all the same technologies we all use daily.
    - We are HUMANS - Tor is made of up a global team of technology, privacy and anonymity experts who are committed to helping preserve freedom of speech online. We are much more than the perception held by some that we are a group of coders in a dark basement somewhere.
    - We build COOL TECH - Tor is a technology and research company - it is not our place to be the moral compass for the people of the world who use any technology.
    - If Tor went AWAY - If Tor were not to exists the many people we help on a daily basis will no longer have access to an important tool which helps to keep them safe and free - but the bad actors will just go find another tool and continue on their path.
    - Beyond our technology and research we actively foster important conversations with many global organizations in order to help people around the world understand the value of privacy and anonymity online.
    - Who uses Tor: Beyond the groups listed on our website we are actively working with individuals and organizations working with victims of domestic violence and cyberstalking to help them understand the tools being used by abusers - making the victim's life miserable and in some cases, fatal. We work with all of the world to journalists to help keep them and their sources safe in areas of the world where surveillance is prevalent and the risks are very real.
    - Who funds Tor: Tor is a non-profit company based in the United States, however, our funding consists of a global user base and global donor base and are listed on our website for people to see for themselves.

Tips and tricks

- Don't overwork or else burnout
- How to manage being a paranoid android.
- Psychological support, with list of people that you can talk to if you feel distressed.
- Gotchas, etc.

Business cards

- Distinction between contractor and employee.

Basic instructions on how to use PGP dongle

What comes with the package

- Stickers and t-shirt included.
- PGP dongle for signing