# Staff Policy

## Background

The IETF Administration LLC (IETF LLC) employs staff both directly and indirectly via an Employer of Record (EOR). The policy provides guidelines to all staff, whether employed directly or indirectly, on various aspects related to their employment.

For those staff employed via an EOR, nothing in this policy can override any policy issued by the EOR, and in the event of a discrepancy between an EOR policy and an IETF LLC policy, then the applicable EOR policy is considered authoritative.

## Hours of working

Staff and the IETF community live in many different time zones, some with limited overlap between each other. This impacts staff in the two key areas of meetings and messaging.

### Meetings

It is not possible to schedule every meeting to be within normal working hours for all participants. Staff are therefore expected to regularly participate in meetings outside of normal working hours and adjust their working schedule accordingly. In general, staff will not be required to participate earlier than 7am or later than 7pm more often than once a week.

### Messaging

It is not possible for someone to check the local timezone of everyone they are messaging to ensure they are only contacting people during the recipients' working hours. Staff are therefore expected to turn off notifications when they are not working, or do not wish to be disturbed, as that allows everyone else to send messages freely without any concern about disturbing a colleague outside of working hours.

## Conduct

This section provides additional guidelines to supplement the IETF LLC Code of Conduct.

## Contractor conduct

If any staff observes unacceptable behavior from a contractor then they are free to address that directly with the person concerned, or raise it with that person's management, they do not need to seek permission from IETF LLC management. This is not meant to imply that staff must address this directly, there remains the option of escalating to IETF LLC management for them to address.

## BCP 25 / RFC 7776 "IETF Anti-Harassment Procedures"

Staff should be aware that BCP 25 / RFC 7776 explicitly includes Staff and therefore staff are free to invoke the anti-harassment procedures and may also be the subject of those procedures.

# Security

## Credentials

All Staff are required, without exception, to manage credentials as follows:

1. Use a password manager for the storage of credentials.
2. Choose passwords with very high entropy, normally no less than 24 characters, unless limited by the system.
3. Not reuse credentials.
4. Use MFA where the system supports it.

## Confidential data

Wherever possible, Staff should store confidential data on the shared corporate infrastructure, such as Google Drive.

If Staff need to maintain local copies of confidential data then the following applies:

- These should either be on encrypted drives or with file level encryption applied.
- They should be regularly reviewed to determine if any can be erased.
- The confidentiality of the data should be protected.