The dataset comes with two protocols: one for developing presentation attack detection (PAD) systems and one for assessing the vulnerability of face recognition.

For PAD, the users are expected to produce a score file for each file in the `bonafide` and `attack` folder and report the Equal Error Rate (EER) metric. No training data is provided.

For vulnerability analysis, two protocols exist: *licit* and *spoof*. In both protocols, users are expected to create models for each identity using the files in `for_models.lst` and probe these models using the files in `for_scores.lst`. In the *licit* protocol, only bonafide samples are in the protocol and in the *spoof* protocol, all probe samples are presentation attacks. Users are expected to report FMR, FNMR, HTER, and IAPMR at EER threshold. Detailed description of the protocol files are available in: https://www.idiap.ch/software/bob/docs/bob/docs/v5.0.0/bob.bio.base/doc/filelist-guide.html

All the metrics are defined in the publication supporting the dataset.