Security implication of building on master

Builds that are run on the master node can read, or modify, files in $JENKINS_HOME. This can be used to perform all sorts of activities that impact the entire Jenkins installation, such as installing plugins, reading credentials, creating new jobs, etc.

In an environment where there’s a distinction between people who administer Jenkins and people who configure jobs or commit changes into projects being built, you should generally configure the master to have no executors, and run builds only on build agents.

If you do not have any other computers to run build agents, or you can run a build agent as a different operating system user on the same computer to achieve the same isolation effect.

Alternatively, use a plugin such as Job Restrictions Plugin to limit which jobs can be run on certain nodes, such as the master, independent of what your less trusted users may use as label expression in their jobs' configurations.