Validation Rules & Field Inventory

Rule ID	Field / Feature	Data Type	Constraints / Rules	Valid Example(s)	Invalid Examples	Error Message	Enforcement Point
VAL-01	Email	String	Must be non-empty, trimmed, match email regex; normalize to lowercase	user@asu.edu	"", abc@, user@@mail	“Please enter a valid email address.”	Registration, Sign in, Change email, Admin invitation
VAL-02	Password	String	8–32 chars; ≥1 uppercase, ≥1 lowercase, ≥1 digit; optional special; not in common/blocked list	PassWord1, Strong!2025	short7, password, 12345678	“Password must be 8–32 chars incl. upper/lower/digit.”	Registration, Sign in, Change password, Admin reset
VAL-03	Name / Username	String	Trimmed; length 3–20; letters/numbers/underscore; must be unique	alex_21, User99	"", a, too_long_username_over_20 chars, bob!	“Username must be 3–20 letters/numbers/underscore, unique.”	Registration, Update profile
VAL-04	Shared Validator API	x	All validations use central helpers (ValidationHelpers) so UI + services apply same rules	x	x	Centralized messages reused everywhere	Across all user/admin flows

New User Feature Validations

Story ID	Fields	Validation
NU-01 Register	Email, Password, Name/Username	Apply VAL-01, VAL-02, VAL-03; enforce uniqueness in DB; password hashed
NU-02 Sign in	Email, Password	Apply VAL-01, VAL-02; safe generic error (“Invalid credentials”)
NU-03 Update Profile	Username	Apply VAL-03; check duplicates
NU-04 Change Password	Current Password, New Password	Current must match DB hash; New must satisfy VAL-02; invalidate old session
NU-05 Change Email	New Email	Apply VAL-01; mark unverified until confirmation

Admin Feature Validations

Story ID	Fields	Validation
ADM-01 List Users	Filter Email / Role	Filter must respect VAL-01 (if email provided) and valid role enum
ADM-02 Activate/Deactivate	Target User ID	Must reference existing user; cannot deactivate self if last admin
ADM-03 Change User Role	Target User ID, Role	Valid role enum; must protect last admin
ADM-04 Reset Password	Target User ID, Temp Password	Temp must satisfy VAL-02; new login forces change

Cross-Cutting Validations

- **XQ-01:** All error messages pulled from a single source (constants or validator API).
- **XQ-02:** Security-sensitive actions (login failure, password change, role change) logged minimally (no PII).
- **XQ-03:** Consistent internal comments/Javadoc across validation functions.