Inledning
Båstad Montessoris verksamhet innefattar daglig hantering av stora informationsmängder. Då vi behandlar både känslig information om individer och information krävs en säker och genomtänkt hantering.
Ansvaret för en bra informationssäkerhet vilar på oss alla inom Båstad Montessori ekonomisk förening både anställda och övriga sysselsatta (såsom konsulter). Denna policy beskriver hur vi ska agera och vilka generella krav som Båstad Montessoris ledning och styrelse ställer på samtliga verksamheter inom föreningen.

Mål och säkerhetsaspekter
Målet för Båstad Montessori ekonomisk förenings informationssäkerhetsarbete är att skydda den information som finns inom verksamheten i syfte att den endast kan användas för det tänkta användningsområdet. Skyddet ska vara anpassat till behoven med avseende på typ, känslighet, risk, lagkrav och andra styrande regelverk eller dokument för våra verksamheter.

Informationssäkerhet inom Båstad Montessori ekonomisk förening utgår från fyra aspekter:
- **Konfidentialitet**: Endast den som för sitt arbete behöver och därför tilldelats behörighet till viss information ska få tillgång till den och ingen annan.
- **Riktighet:** Information ska inte förändras genom misstag, obehörig tillgång eller tekniska fel.
- **Tillgänglighet:** Information ska kunna nås och användas av de som är behöriga inom önskad tid och från rätt plats.
- **Spårbarhet:** Bearbetning av och åtkomst till väsentlig information ska kunna spåras.

Det gäller också att noga avgöra om information är konfidentiell eller känslig ur något perspektiv, om det inte är så ska vi eftersträva att vara så transparenta som möjligt.

Övergripande roller och ansvar
Samtliga medarbetare, och andra sysselsatta i Båstad Montessori ekonomisk förenings verksamheter, har ansvar för att hantera information korrekt. Ytterst vilar ansvaret på den som är informationsägare, styrelsen som representant för huvudmannen. Ansvaret kan delas upp och delegeras vid behov. De huvudsakliga konfidentiella och känsliga informationsområden som Båstad Montessori ekonomisk förenings hanterar listas nedan med sina respektive informationsägare:

- Personuppgifter om barn, elever, vårdnadshavare, deltagare, kunder och samarbetspartners - *Verksamhetens tillståndspliktiga huvudman dvs styrelsen. - Generell delegation till rektor för vår skolverksamhet och till förskolechef inom förskolorna samt ekonomichef.*
- Personuppgifter om anställda, såsom löneuppgifter, behörighetsinformation och övriga personalnyckeltal – *ekonomichef och respektive chef (rektor/ förskolechef).*

- Ekonomisk information – *ekonomichef och ansvarig chef (rektor/ förskolechef)*
- Kommersiella anbud och konfidentiella avtal – *ekonomichef och ansvarig chef (rektor/förskolechef)*
- Riskrapportering, tillsynslogg samt anmälningar – *ansvarig chef (rektor/ förskolechef)*

En stor del av vår information lagras i för ändamålet avsedda IT-system för vilka det ofta finns en utsedd systemägare.

Riskbedömning och riskhantering
Det åvilar respektive informationsägare och systemägare att regelbundet genomföra riskbedömningar och hantera de informationsrisker som identifieras. I de fall man upptäcker brister eller risker avseende informationssäkerhet ska överordnad funktion/ansvarig omgående informeras på ett tydligt sätt och åtgärder vidtas, enligt gällande lagstiftning.

Informationssystem (IT)
Mycket av verksamhetens information finns i digitala system och arkiv. Det är därför viktigt att processer runt tillgång och behörigheter är väl definierade. Även informationssäkerhet i form av backuper är väsentligt.

Tillgång: tillgången till IT-baserade system sker via användarkonton. Konton ska vara personliga vid hantering av väsentlig information för att möjliggöra spårbarhet. Konton ska endast skapas efter beställning och godkännande av närmsta chef.
Varje system- och informationsägare ska säkerställa att säkerhetsnivån för inloggning (autentisering) motsvarar känsligheten i den information som lagras i respektive system. Även säkerhetskrav på lösenord bör följa detta.
Varje chef är personligen ansvarig att säkerställa att konton beställs, uppdateras och avbeställs för medarbetare när dessa börjar, byter eller avslutar sin anställning.

Behörigheter: behörigheter till olika funktioner och information ska endast ges till dem som behöver detta i sitt arbete och kan ges efter beställning och godkännande av respektive informationsägare eller på dennes delegation. Behörighet till centrala ekonomi-, faktura- och personalsystem ska tilldelas enligt fastslagen rutin.
Samtliga ärenden rörande tillgång och behörigheter ska vara spårbara och dokumenteras i ärendehanteringssystem. Varje informationsägare och systemägare ska säkerställa att det minst en gång per år görs en översyn av behörigheterna i respektive system.

Antalet personer med höga behörigheter (så kallade fulla administratörs-rättigheter) ska begränsas så långt det går. Höga behörigheter får endast användas för att fullgöra nödvändiga arbetsuppgifter kopplade till ärenden och problem.
Lagring: Det åligger respektive systemägare att säkerställa att information säkerhetskopieras och arkiveras enligt god praxis samt gällande lagar och regler.

Personligt ansvar för informationssäkerhet
Utgångspunkten är att varje individ är ansvarig för att hålla sina lösenord och IT-utrustning säker. Varje individ är också ansvarig för att lagra, behandla information enligt gällande direktiv.
Just lösenord är en viktig del av vår digitala säkerhet och ska aldrig lämnas ut till annan person.
Lösenord som används till Båstad Montessoris system får inte användas i något annat system eller tjänst då det kraftigt ökar risken för intrång. Om vi lämnar dator/platta/telefon utan övervakning ska den låsas eller stängas av så att obehörig åtkomst förhindras.
Förlust av utrustning eller misstanke om obehörigt användande av lösenord eller annan åtkomst ska anmälas direkt till expeditionen som kontaktar IT-ansvarig.

Dessa medarbetare ska intyga och följa de riktlinjer som finns i "Riktlinje för skydd av mobila enheter". Utgångspunkten är att detta gäller samtliga.

Informationsklassificering och utskrifter
I samband med hantering av projekt med kurspåverkande information, som exempelvis förvärv, ska rutiner gällande loggbok och sekretessförbindelser följas.

Känsliga personuppgifter
Känsliga personuppgifter (exempelvis information om hälsa eller facklig tillhörighet) eller personuppgifter som kan uppfattas som integritetskänsliga (exempelvis löneuppgifter, barns utveckling eller pedagogiska utredningar) ska alltid hanteras med extra varsamhet och i system/lösningar anpassade till detta. Inloggning till dessa system/lösningar ska i normalfallet ske med säker inloggning (tvåfaktorsinloggning). Båstad Montessoris Dataskyddspolicy beskriver hantering av personuppgifter i mer detalj.
Varje vårdgivare, anlitade av Båstad Montessori ekonomisk förening, ska ha ett väldokumenterat ledningssystem som tydligt anger ansvaret för medicinska och psykologiska insatserna samt innehåller en Informations-säkerhetspolicy. Informationssäkerhetspolicyn ska stämmas av med huvudmannen, eller av denne utsedd person, och efterlevnaden ska regelbundet följas upp av ansvarig inom verksamheten.

Finansiell information
Båstad Montessori ekonomisk förenings centrala ekonomisystem innehåller både väsentlig och känslig information om föreningens verksamhet.
Systemen omfattas därför av höga krav på behörighetshantering och åtkomst. Åtkomst kräver att man är uppkopplad via Båstad Montessoris nätverk eller via VPN (Virtual Private Network) för åtkomst.
Finansiell information av känslig eller väsentlig natur får endast sändas med epost som krypterad bilaga där nyckeln lämnas ut på annat sätt än epost (ex SMS). Personer som löpande arbetar med sådan känslig finansiell information ska ha datorer och telefoner utrustade med krypterad lagring samt iaktta extra vaksamhet med sina digitala arbetsredskap.

Fysiskt arbetsmaterial med väsentlig information hanteras genom att personer i insynsställning ska låsa in sådana utskrifter och att deras arbetsplatser ska förses med lås på dörrar.

T-infrastruktursäkerhet
Ytterst ansvarig för IT-säkerheten är huvudmannen för Båstad Montessori ekonomisk förening. Huvudmannen kan delegera detta till utsedd person. I ansvaret ingår säkerhet i form av relevanta brandväggar som skydd mot intrång och grundläggande skydd för information som lagras i system inom Båstad Montessoris centrala driftsmiljö. Det ingår även i ansvaret att säkerställa att leverantörer av centralt upphandlade IT-tjänster svarar upp mot föreningens krav på informationssäkerhet avseende både data och fysisk säkerhet (skydd av datahallar).
Båstad Montessori ekonomisk förening har ett ansvar att säkerställa att de kommunikationslösningar som används inom föreningen uppfyller en marknadsmässig nivå vad avser kommunikationssäkerhet och tillgänglighet.

Övervakning och loggar
Systemägare ansvarar för kravställande av övervaknings- och loggnings-funktioner för respektive system utifrån aktuell behovsbild.
Vid inhämtning av information av utredningskaraktär, dvs utan individens explicita samtycke, ska alltid föreningens ordförande meddelas och minst två personer med olika funktion (exempelvis närmsta chef samt HR-representant) agera ihop för att säkerställa en bra hantering och därmed även skydda enskilda individer från eventuellt missbruk.

Respektive informationsägare och systemägare är ansvarig för att hantera och följa upp eventuella säkerhetsincidenter och åtgärda dessa skyndsamt samt vidta åtgärder för att minska dess konsekvenser.
I de fall då verksamheter eller personer kan påverkas ska relevant chef involveras från berörd verksamhet. Är incidenten av polisiär eller annan allvarlig natur ska ordförande för föreningen involveras. Relevant chef ska alltid informeras vid incidenter som inte är av trivial karaktär. I det fall en incident gäller integritetskänsliga eller känsliga personuppgifter ska detta dessutom meddelas skyndsamt, vartefter hen beslutar om rapportering till Datainspektionen ska göras.
Om en incident riskerar att påverka Båstad Montessoris verksamhet (helt eller i delar) på ett affärsmässigt sätt ska verksamhets krisledning samt föreningens styrelse involveras.

Uppföljning och revision
I samband med den årliga revisionen granskas även IT-området och uppföljning av informationssäkerheten sker via genomgångar med berörda, samt genom uppföljning av specifika ärenden.

Denna policy har fastställts av Båstad Montessoris styrelse. Grevie den XXXXX